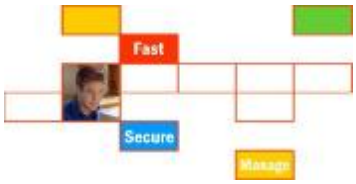
Microsoft
Internet Security
and Acceleration
Server



ISA Server 2004 EE Common Criteria Evaluation

Security Target

Internet Security and Acceleration Server Team

Author:	Stephan Slabihoud, TÜVIT GmbH Ben Bernstein, Microsoft Corp.
Category:	CC Evaluation
Status:	Final
Version:	1.1
Revision:	1
Last Saved:	2006-05-11
File Name:	MS_ISAEE_ST_1.1.doc

Abstract

This document describes the ST (Security Target) of ISA Server 2004 EE Common Criteria Certification that is the basis for the ISA Server 2004 EE CC evaluation.

Keywords

CC, ST, Common Criteria, Firewall, Security Target

Revision History

Date	Version	Author	Edit
20-Mar-06	0.1	Stephan Slabihoud Ben Bernstein	Created
07-Apr-06	1.0	Stephan Slabihoud Ben Bernstein	Some changes according EE
11-May-06	1.1	Stephan Slabihoud Ben Bernstein	Feedback from evaluation body added

This page intentionally left blank

Table of Contents

List of Tables

Page

List of Figures

Page

1 Introduction

This chapter contains document management and overview information. The Security Target (ST) identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a ST. The ST overview summarizes the ST in narrative form and provides information for a potential user to determine whether the ISA Server 2004 is of interest. The overview can also be used as a standalone abstract for ST catalogues and registers.

1.1 Identification

The title of this ST is “ISA Server 2004 EE Common Criteria Evaluation - Security Target”, Version 1.0, Revision 1, dated 2006-04-07.

The Target of Evaluation (TOE) is a dedicated software firewall called “Microsoft Internet and Acceleration Server 2004 – Enterprise Edition – Service Pack 2”. Its version is MS ISA Server 2004 Enterprise Edition - 4.0.3443.594 (including documentation).

The Security Target is built in accordance with Common Criteria V2.1 with Final Interpretations [CC].

1.2 Overview

This chapter presents a general overview of the Microsoft Internet Security and Acceleration Server 2004 EE[1].

ISA Server 2004 is a firewall that helps to provide secure Internet connectivity. ISA Server 2004 is an integrated solution optimized for application-layer defense, stateful packet inspection (SPI), and secure web publishing. Microsoft ISA Server 2004 introduces multi-networking support, virtual private networking configuration, extended and extensible user and authentication models, and improved management features.

ISA Server 2004 can be installed as a dedicated (software) firewall that runs on Windows 2003 Server operating system. It acts as the secure gateway to the Internet for internal clients and protects communication between internal computers and the Internet.

As a multilayered firewall, ISA Server 2004 provides security at different levels. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application-level filtering allows ISA Server 2004 to intelligently inspect and secure popular protocols (such as HTTP, and others). ISA Server 2004 also performs dynamic-filtering using stateful packet inspection (SPI) to open communication ports only when requested by clients and close them when they are no longer needed. This reduces the number of communication ports that are statically open to inbound connections.

[1] short: „ISA Server 2004“

With ISA Server 2004's filtering capabilities, it is possible to create a rule that allows or denies traffic on the packet layer and with data-aware filters to determine if packets should be accepted, rejected, redirected, or modified. ISA Server 2004 has built in identification and authentication capabilities which can be configured separately for incoming and outgoing requests. The firewall features detailed 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.

There are two versions of ISA Server 2004 available: Standard Edition (single machine support only) and Enterprise Edition (for large-scale deployments). Chapter 2.1.1 describes the differences between both versions.

1.3 Related Documents

Related documents are:

- Microsoft Internet Security and Acceleration Server 2004 EE manual [MSISA]
- Common Criteria for Information Technology Security Evaluation [CC]

The main chapters of the ST are the TOE Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, PP Claims and Rationale.

Chapter 2, the TOE Description, provides general information about the TOE, serves as an aid to understanding the TOE's security requirements, and provides context for the ST's evaluation.

The TOE Security Environment in Chapter 3 describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

a) Assumptions regarding the TOE's intended usage and environment of use
b) Organizational Security Policies (OSP)
c) Threats relevant to secure TOE operation

Chapter 4 contains the security objectives that reflect the stated intent of the ST. The objectives define how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

Chapter 5 contains the applicable security requirements taken from the Common Criteria, with appropriate refinements. The requirements are provided in separate subsections for the TOE and its environment. The IT security requirements are subdivided as follows:

a) TOE Security Functional Requirements
b) TOE Security Functional Requirements
c) TOE Security Functional Requirements for the IT Environment

The TOE summary specification in chapter 6 defines the security functions and the assurance measures.

The security target does not claim for compliance with any existing protection profile (see Chapter 7).

The Rationale in Chapter 8 presents evidence that the ST is a complete set of requirements and that the TOE provides an effective set of IT security countermeasures within the security environment.

The rationale is divided in three main parts:

- A security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them,
- A security requirements rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them, and
- The TOE summary specification rationale consists of a TOE security functions rationale and an assurance measures rationale.

A glossary of acronyms and terms used in the ST as well as references are provided in the Appendix in chapter 9.

1.4 Common Criteria Conformance

This ST has been built with Common Criteria (CC) Version 2.1 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements). The TOE itself is conformant with Common Criteria Version 2.1, part 2 and part 3 [CC].

This security target does not claim for compliance with any existing protection profile.

The assurance level for the TOE is **EAL 4 augmented (augmented with AVA_VLA.3 and ALC_FLR.1)**. There is no SOF claim within the TOE.

2 ISA Server 2004 and TOE demarcation

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives, and security functional requirements can be employed.

Chapter 2.1 refers to the particular TOE implementation. Chapter 2.2 describes additional features that are not part of the TOE.

2.1 TOE overview

The TOE is the main part of ISA Server 2004 (the logical scope and boundary are described in chapter 2.1.3). It is a firewall that helps to provide secure Internet connectivity. The TOE is an integrated solution for application-layer defense, stateful packet inspection, and secure web publishing. The TOE can be installed as a dedicated (software) firewall that runs on Windows 2003 Server operating system. As a multilayered 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 the TOE to inspect and secure protocols (such as HTTP, and others). The TOE also performs dynamic-filtering using stateful packet inspection to open communication ports only when requested by clients and close them when they are no longer needed.

The operation system Windows 2003 Server maintains security attributes for all administrators. Windows 2003 Server 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 next chapters describe the physical scope and boundary and the basic functionalities of the TOE.

2.1.1 Available product versions

There are two versions of ISA Server 2004 available: Standard Edition (single machine support only) and Enterprise Edition (for large-scale deployments).

The Enterprise edition is designed for large-scale deployments with high-volume Internet traffic environments. It supports multi-server arrays with centralized management as well as enterprise-level and array-level security policy. Enterprise Edition has no hardware limits. ISA Server 2004 Standard Edition shares the feature set of Enterprise Edition, but it is intended for small businesses, workgroups, and departmental environments. Standard Edition provides local policy only, and supports up to four processors.

For the Standard Edition security policy configuration data is stored in the local Windows registry, for the Enterprise Edition security policy configuration data is stored in ADAM (a

Lightweight Directory Access Protocol (LDAP) directory service)[2]. The configuration data is then replicated by a system service into the local Windows registry and file system. Network Load Balancing, which is also a feature of the Enterprise Edition, is designed to work as a standard networking device driver in the Windows Server 2003 and not started by default.

Both versions - Standard and Enterprise - can be treated the same way because the storage of policy configuration data is not part of the evaluation (Windows Registry and ADAM with the ADAM configuration receiver service are outside the scope of the TOE) and also scalability is not part of the evaluation.

The Enterprise Edition with local administration (which means that ADAM is located on the same machine as the TOE) has been chosen as TOE.

2.1.2 Physical scope and boundary

The TOE is delivered in a package which consists of:

- The software package “Microsoft Internet and Acceleration Server 2004 – Enterprise Edition – Service Pack 2” installed running on a single machine, which comprises the evaluated TOE and non evaluated components.
- A manual (a Windows Help File), which is delivered as part of the software package and installed on the host system with the TOE

The TOE is running on an

- certified Windows Server 2003 Standard Edition (English) SP1 including MS05-042 (KB899587), MS05-039 (KB899588), MS05-027 (KB896422), and patch KB907865 (same installation that has been used for Windows 2003 Server Common Criteria EAL 4+ Evaluation; Validation Report Number CCEVS-VR-05-0131, [WINST] and [WINVR])

which has been used as underlying operating system for evaluation.

The evaluated functionality respectively the TOE (the logical scope) is stated in the following chapter 2.1.3. In particular Figure 2.1 shows the demarcation of the TOE respectively ISA Server 2004.

[2] http://www.microsoft.com/windowsserver2003/adam/default.mspx

2.1.3 Logical scope and boundary

The logical scope and boundary of the TOE is subdivided into the following major functions of the TOE:

- Web Identification and Authentication,
- Filtering (Information Flow Control) and
- Audit.

2.1.3.1 Web Identification and Authentication

The web publishing rules[3] of the TOE can be configured to allow or deny a set of computers[4] or a group of users to access specific servers. If the rule applies specifically to users, the TOE checks how the user should be authenticated. It is possible to configure incoming and outgoing Web request settings so that users must always be authenticated by the TOE. This ensures that requests are allowed only if the user making the request is authenticated. It is possible to choose between different authentication methods also separately for incoming and outgoing requests.

The TOE supports Basic authentication which is the standard method of authentication for Hypertext Transfer Protocol (HTTP) transmissions. Basic authentication sends and receives user information as text characters. No encryption is used with basic authentication.

The TOE also supports OWA Form Based Authentication[5], which is a filter for form based authentication for Outlook Web Access.

The TOE is configured that it supports Basic authentication or OWA only. Basic authentication for web requests or OWA can be secured using an SSL channel, so user identification and authentication credentials are encrypted during transmission. The TOE allows verifying the user credentials either by asking the local user database or an external RADIUS server.

2.1.3.2 Filtering (packet and application level filtering)

The TOE combines several security mechanisms to enforce the security policies at different network layers: a rule base for enforcing policies between any two networks, application filters, and system security configuration options.

The TOE distinguishes between the following types of rules:

[3] see chapter 2.1.3.2 and glossary

[4] „client address set“ or „client set“

[5] basically this filter intercepts HTTP traffic and displays a HTTP web page that allows the user to enter the user credentials

Firewall Policy rules:

Firewall policy rules specify whether traffic is allowed to pass between networks. The TOE defines the following types of rules:

Access rules

Define whether traffic from the source network is allowed to pass to the destination network.

When a client requests an object using a specific protocol, the TOE checks the access rules. A request is processed only if an access rule specifically allows the client to communicate using the specific protocol and also allows access to the requested object.

Web publishing rules

Define whether requests from the destination network are allowed for Web servers on the source network.

The TOE uses Web publishing rules to relieve the concerns associated with publishing Web content to the Internet without compromising internal network security. Web publishing rules determine how the TOE should intercept incoming requests for HTTP objects on an internal Web server and how the TOE should respond on behalf of the Web server. Requests are forwarded downstream to an internal Web server, located behind the TOE. If possible, the request is serviced from the ISA Server 2004 cache (which is not evaluated).

Web publishing rules essentially map incoming requests to the appropriate Web servers behind the TOE.

Server publishing rules

Define whether requests from the destination network are allowed for resources on the source network.

The TOE uses server publishing to process incoming requests to internal servers. Requests are forwarded downstream to an internal server, located behind the TOE.

Server publishing allows virtually any computer on your internal network to publish to the Internet. Security is not compromised because all incoming requests and outgoing responses pass through the TOE. When a server is published by the TOE, the IP addresses that are published are actually the IP addresses of the TOE (NAT relationship).

Mail publishing rules

Strictly speaking this is not a special kind of rule; it is a different wizard that helps the user to create an appropriate Server publishing rule. In the Security Function 2 (chapter 6.1.2) both rules – Server publishing rules and Mail publishing rules – are treated the same way.

Define whether requests from the destination network are allowed for mail servers on the source network. The TOE uses Mail publishing rules to publish E-Mail servers to the Internet without compromising internal network security. Mail publishing rules determine how the TOE should intercept incoming E-Mails to an internal E-Mail server. Requests are forwarded downstream to an internal E-Mail server, located behind the TOE.

Mail publishing rules essentially map incoming requests to the appropriate Mail servers behind the TOE.

Web- and Application filters:

ISA Server 2004 application filters provide an extra layer of security. Web- and Application filters can access the datastream or datagrams associated with a session. Web- and Application filters are registered with the Firewall service (a service installed by ISA Server 2004) and work with some or all application-level protocol streams or datagrams. A Web- and Application filter can perform protocol-specific or system-specific tasks, such as authentication and virus checking.

Web- and Application filters differ according to the supported protocols. Filters, which intercept the HTTP protocol are called Web filter, all other protocols are called Application filter in ISA Server 2004.

Web filters supported by the TOE are: HTTP (web proxy filter) and OWA.

Application filters supported by the TOE are: FTP, RPC and SMTP.

Network rules (route and NAT):

It is possible to configure network rules in the TOE, thereby defining and describing a network topology. Network rules determine whether there is connectivity between two networks, and what type of connectivity is defined. Networks can be connected in one of the following ways: Network address translation (NAT) and Route.

System policy:

The TOE protects network resources, while connecting them securely for specifically defined needs. The TOE introduces a system policy, a set of firewall policy rules that control how the TOE enables the infrastructure necessary to manage network security and connectivity. The TOE is installed with a default system policy, designed to address the balance between security and connectivity.

2.1.3.3 Audit

The TOE features detailed security and access logs (firewall service log file and web proxy log file). For evaluation the MSDE log file is used for which the TOE offers no additional access protection (the access protection is granted by the file system of the underlying operation system).

The TOE provides the ability to perform filter operations on the recorded audit data. It is also possible to sort the audit trail.

2.1.3.4 TOE demarcation summary

For better understanding the boundaries of the TOE are summarized in Figure 2.1. It shows the TOE with its three main security functionalities:

- Web Identification & Authentication,
- Information Flow Control, and
- Audit,

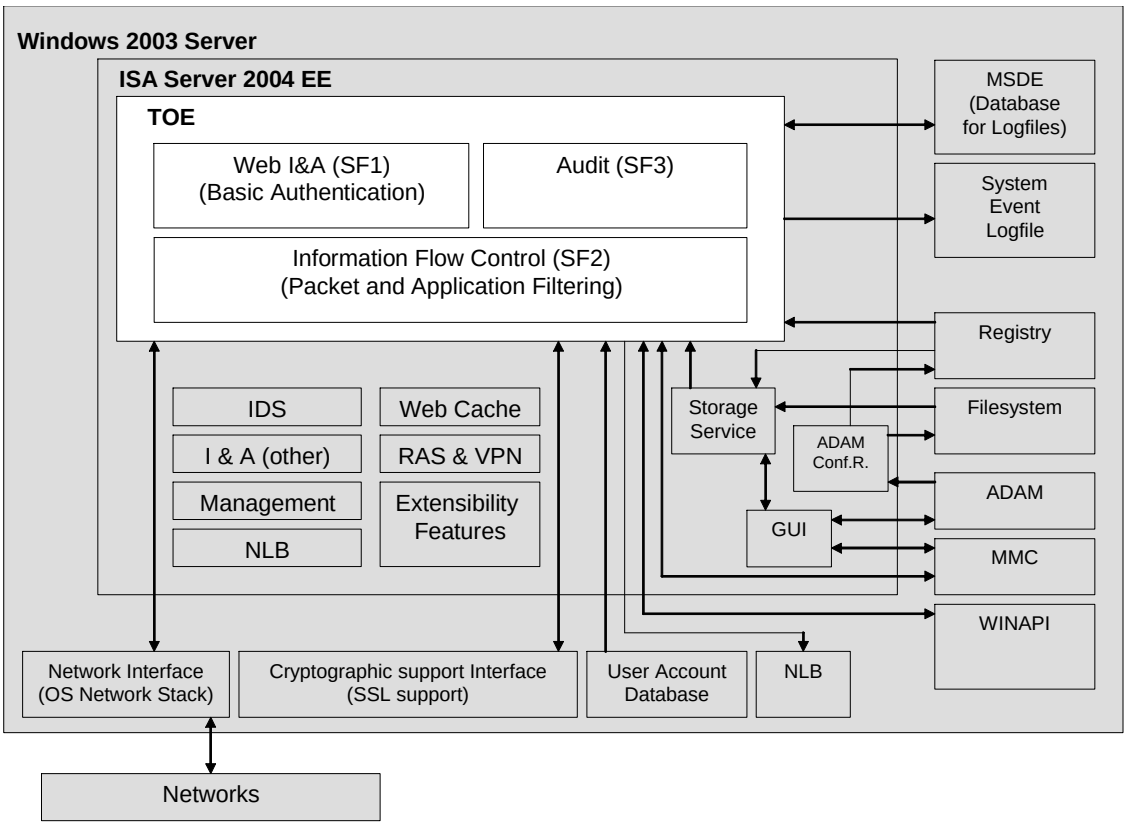
the additional features of the ISA-Server which are not part of the evaluation: Web Cache, GUI (except Log Viewer component), RAS & VPN, Storage Service, ADAM Configuration Receiver, IDS, Load Balancing, other Management and Identification & Authentication functionality, Extensibility Features, some protocol filters (not mentioned in the picture above) and the used functionalities of the underlying operating system Windows 2003 Server. The arrows show the interfaces between the TOE and the operating system, the arrowheads show the direction of possible information flow. The TOE uses the MSDE database and the event log file to store the audit data, which is protected for unauthorized access by the file system. The configuration is read from the registry and file system using the Storage Service, which has been replicated from ADAM to the registry and file system using the ADAM Configuration Receiver Service. The user account database provides the information required by the Web I&A functionality of the TOE. The cryptographic support interface supports the SSL functionality. The network interface is needed for transmitting data to the different networks. The interface to the MMC is required since one component of “Audit” (SF3) uses this interface to display log data (Log Viewer component). The Windows API (WinAPI) provides low level functions which are used by the TOE. The Network Load Balancing functionality of the underlying operating system is also provided to ISA Server 2004 EE.

For information purpose and better understanding the interfaces between

- GUI and Storage Service, MMC & ADAM,
- Storage Service and Registry & Filesystem, and
- ADAM Configuration Receiver and ADAM, Filesystem & Registry,

are also shown in the picture below.

Figure 2.1 – TOE demarcation



ADAMConf.R. = ADAM Configuration Receiver

2.2 ISA Server 2004 EE overview

Though the TOE is the main part of ISA Server 2004 EE, it comprises the three security functions only. This chapter gives a short overview about the complete functionality of ISA Server 2004 EE. The following table gives an overview about the features of ISA Server 2004 EE.

Table 2.1 – ISA 2004 EE Features at a Glance

Feature	Functionality
Firewall and Security Features	
Multilayered firewall security[6]	Provides filtering at the packet, circuit and application levels for multi-layered protection. Includes spam control capability via e-mail filtering of keywords and attachments.
Secure e-mail	Provides secure RPC filtering for remote Outlook users and enhanced

[6] ISA Server 2004 uses a new architecture compared to ISA Server 2000 (new services; no separation between Firewall Service and Web Proxy Service).

	security for Outlook Web Access (OWA).
Policy based access control	Allows organizations to control inbound and outbound access by user/group, application, source/destination, content type and schedule.
Stateful inspection and stateful filtering	Examines data at the firewall in relation to protocol and connection state. Dynamic packet filtering means ports are opened only when necessary.
Integrated VPN	Provides secure site to site and remote access VPN connections over PPTP, L2TP/IPSec and IPSec tunnel mode protocols.
Integrated intrusion detection	Protects against common network attacks and allows configuration of alerts
Advanced authentication	Uses Windows authentication (NTLM, Kerberos), digital certificates, Remote Authentication Dial-in User Service (RADIUS)
Availability	
Load Balancing	Windows Network Load Balancing (NLB) support
Fast, Secure Web Caching and Web Proxy Features	
High performance forward and reverse caching	Accelerates Web performance both for internal users accessing the Internet and external users accessing internal Web servers.
Caching scalability	Provides for easy scaling up via Cache Array Routing Protocol (CARP) and dynamic network load balancing.
Distributed and hierarchical caching	Allows configuration to place caches near users or in chained configurations, with multiple and backup routes.
Active caching	Automatic refresh of popular content optimizes bandwidth usage.
Scheduled content download	Ensures efficient use of the network by distributing content and preloading cache on a predefined schedule.
Management and Extensibility Features	
Simplified Management	Intuitive console interface (GUI), graphical taskpads and Wizards make many common tasks point-and-click. Firewall configuration can be copied to an XML file for standardization or backup.
Remote management	ISA Server can be remotely managed via the MMC console, the Windows 2000 Terminal Services or the Windows Server 2003 Remote Desktop, as well as command-line scripts. Secure SSL/RDP tunneling can be used when ISA Server 2004 is installed on Windows Server 2003.
Logging, Reporting and Alerts	Provides detailed security and access logs in standard formats (delimited text, MSDE, SQL database). Reports can be automatically published to local folders or remote file shares. Alerts can e-mail administrators or take automated actions.
Enterprise policies	Array and enterprise policies use Active Directory Application Mode (ADAM)

The access policy[7] and publishing rules[8] of the TOE can be configured to allow or deny a set of computers[9] or a group of users to access specific servers. Additionally to the evaluated authentication method mentioned in chapter 2.1.3.1 ISA Server 2004 supports following authentication methods:

[7] see chapter 2.1.3.2 and glossary

[8] see chapter 2.1.3.2 and glossary

[9] „client address set“ or „client set“

- Digest authentication
- Integrated Windows authentication
- RSA SecurID Authentication
- SSL certificate authentication (Client certificates and server certificates)
- Radius authentication

Delegation of authentication helps increase security by enabling ISA Server 2004 to authenticate Internet clients instead of passing the pre-authentication to the published server. This delegation also eliminates multiple login prompts. Delegation is possible with SecurID and Basic (user name and password) authentication and can be enabled for each Web publishing rule.

ISA Server 2004 combines several security mechanisms to enforce the security policies at different network layers: a rule base for enforcing policies between any two networks, application filters, and system security configuration options.

Except the features mentioned in chapter 2.1.3.2 ISA Server 2004 EE supports following:

- An internal web cache (ISA cache), which can answer HTTP requests instead of requesting the object from a web server.
- Various application filters, like: DNS, H.323, MMS, PNM, POP[10], PPTP, RTSP, and SOCKSv4.
- Various web application filters, like: HTTP Compression, DiffServFilter (quality of service for HTTP traffic), Link Translation Filter.

ISA Server 2004 features detailed security and access logs (firewall service log file and web proxy log file), which can be generated in standard data formats like W3C[11]. The log files are stored locally in human readable text files[12], in an ODBC database or in a MSDE database (which is the evaluated method). It is possible to change the destination folder the text log files are created in. ISA Server 2004 offers no additional access protection for the log files. Access protection is granted by the file system of the underlying operation system. The MSDE database provides additional access control that is also not done by ISA Server 2004.

[10] intrusion detection filter, checks for POP buffer overflow attacks

[11] http://www.w3.org/Daemon/User/Config/Logging.html

[12] ISA Server can store log files locally or remote in a database. The ISA Server reporting system centralizes the logs, collecting data from all the servers into a single report. This feature is not part of the TOE.

3 TOE Security Environment

This chapter aims to clarify the security problems that the ISA Server 2004 is intended to solve, by describing any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used and any known or assumed threats to the assets against which protection within the TOE or its environment is required. This is done considering the attack potential of attackers aiming to discover exploitable vulnerabilities to be medium.

3.1 Assumptions

Table 3.1 lists the TOE Secure Usage Assumptions for the IT and non-IT environment and intended usage.

Table 3.1 – Assumptions for the IT and non-IT Environment and intended usage

#	Assumption Name	Description
1	A.DIRECT	The TOE is available to authorized administrators only. Personnel who has physical access to the TOE and can log in the operating system is assumed to act as an authorized TOE administrator.
2	A.GENPUR	The TOE stores and executes security-relevant applications only. It stores only data required for its secure operation. Nevertheless the underlying operating system may provide additional applications required for administrating the TOE or the operating system.
3	A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
4	A.ENV	The environment implements following functionality: local identification and authentication of user credentials used for web publishing (see A.WEBI&A for Radius identification and authentication; in case of a successful authentication the TOE analyses the returned value and allows or denies the access to network resources depending on that value), reliable time stamp (log file audit), file protection (for log file access protection, registry protection, and ADAM protection), cryptographic support (for SSL encryption), administration access control, reliable ADAM implementation, Network Load Balancing (disabled by default).
5	A.PHYSEC	The TOE is physically secure. Only authorized personal has physical access to the system which hosts the TOE.
6	A.SECINST	Required certificates and user identities are installed using a confidential path.
7	A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

8	A.WEBI&A	User credentials are verified by a Radius Server. The Radius Server returns a value if a valid account exists or not. Web Identification & Authentication with a Radius Server requires that the Radius server is placed on the internal network, so that data (user credentials and return values) transferred to and from the Radius Server is secured by the TOE from external entities.
9	A.SSL	All web publishing rules which support Basic authentication have to be configured by the administrator so that strong encryption for SSL is enforced (at least 128bit encryption).

3.2 Organisational Security Policies

Security policies to be fulfilled by the TOE are defined in Table 3.2 below.

Table 3.2 – Security Policies addressed by the TOE

#	Policy Name	Description
1	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.

3.3 Threats

Threats to the TOE are defined in Table 3.3 below. The asset under attack is the information transiting the TOE. In general, the threat agent (attacker) includes, but is not limited to:

1) not authorized persons or

2) external IT entities not authorized to use the TOE itself.

Table 3.3 – Threats

#	Threat	Description
1	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. The TOE provides Basic Authentication. An attacker might exploit a security flaw in this Authentication scheme implementation to get access to e.g. protected web pages.
2	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. Impermissible information might be corrupted packets, invalid or nonstandard http headers, or in general invalid requests that exploit the TOE's security functions (the TOE might be inoperable after such exploitation or reveal protected information).

3	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. This flaw might be a result of not initialized buffers.
4	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. This might be a result of a strange denial of service attack.

4 Security Objectives

4.1 Security Objectives for the TOE

TOE security objectives are defined in Table 4.1, below.

Table 4.1 – Security Objectives for the TOE

#	Objective	Description
1	O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions that require authorization for certain specified services defined by the firewall rule set (e.g. a web publishing rule that requires Basic Authentication). The TOE has to request user credentials from the user and has to call a function in the operating system/Radius Server to verify these.
2	O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.
3	O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
4	O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail. The TOE ensures that no records are left because of not enough storage capacity.
5	O.ACCOUN	The TOE must provide user accountability for information flows through the TOE.

4.2 Security Objectives for the Environment

Table 4.2 lists security objectives for the Environment (covers objectives for the IT-Environment and non IT-Environment).

Table 4.2 – Security Objectives for the Environment

#	Objective Name	Objective Description
1	OE.DIRECT	The TOE should be available to authorized administrators only.
2	OE.GENPUR	The environment should store and execute security-relevant applications only and should store only data required for its secure operation.
3	OE.NOEVIL	Authorized administrators should be non-hostile and should follow all administrator guidance.

#	Objective Name	Objective Description
4	OE.ENV	The environment should implement following functionality: local identification and authentication of user credentials used for web publishing (see OE.WEBI&A for Radius identification and authentication; in case of a successful authentication the TOE analyses the returned value and allows or denies the access to network resources depending on that value), reliable time stamp (log file audit), file protection (for log file access protection, registry protection, and ADAM protection), cryptographic support (for SSL encryption), administration access control, reliable ADAM implementation, Network Load Balancing (disabled by default).
5	OE.PHYSEC	The system which hosts the TOE should be physically secure.
6	OE.SECINST	The required user identities (used for user authentication) and required SSL certificates for server authentication (HTTPS encryption) should be stored using a confidential path. That means that created certificates and user passwords should not be available to unauthorized persons (OE.DIRECT ensures that unauthorized persons cannot get these information by accessing the TOE).
7	OE.SINGEN	Information should not flow among the internal and external networks unless it passes through the TOE. Thereby the TOE administrator has to guarantee an adequate integration of the TOE into the environment.
8	OE.WEBI&A	The Radius Server should verify provided user credentials and return if a valid account exists or not. Data (user credentials and return values) between TOE and the Radius Server should be transferred in the TOE secured environment, which means that the Radius Server should be placed on the internal network for Web Identification & Authentication.
9	OE.SSL	All web publishing rules which support Basic authentication should be configured by the administrator so that strong encryption for SSL is enforced (at least 128bit encryption).

5 IT Security Requirements

5.1 Introduction

This chapter defines the TOE security functional requirements and assurance requirements. All requirements are taken from the CC Parts 2 and 3, except the functional requirements prefixed with “EXT_”, which are not explicitly taken from CC part 2 but which rely on the functional requirements in CC part 2. These extended functional requirements have been used to avoid confusion with the “classical” identification and authentication used in CC. Selections, assignments, and refinements performed are indicated by *italics* and stated which operation is used.

5.2 TOE Security Functional Requirements

This chapter defines the TOE security functional requirements. A list of the requirements is provided in Table 5.1. The full text of the security functional requirements is contained below. Certain security functional requirements have multiple iterations in the text. Iterations are indicated by the use of parentheses “()” in the component identification and by parentheses “()” and an abbreviation in the component name.

Table 5.1 – TOE Security Functional Requirements

#	Functional Requirement	Title	Dependencies
Audit			
1	FAU_GEN.1	Audit data generation	FPT_STM.1
2	FAU_SAR.1	Audit review	FAU_GEN.1
3	FAU_SAR.3	Selectable audit review	FAU_SAR.1
4	FAU_STG.3	Action in case of possible audit data loss	FAU_STG.1
Web Identification & Authentication			
5	EXT_FIA_AFL.1	Authentication failure handling	EXT_FIA_UAU.2
6	EXT_FIA_UID.2	User identification before any action	none
7	EXT_FIA_UAU.2	User authentication before any action	EXT_FIA_UID.2
Information Flow Control			
8	FDP_IFC.1 (1)	Subset information flow control (1) - UNAUTHENTICATED SFP	FDP_IFF.1 (1)
9	FDP_IFC.1 (2)	Subset information flow control (2) - UNAUTHENTICATED_APPL SFP	FDP_IFF.1 (2)
10	FDP_IFC.1 (3)	Subset information flow control (3) - AUTHENTICATED SFP	FDP_IFF.1 (3)
11	FDP_IFF.1 (1)	Simple security attributes (1) - UNAUTHENTICATED SFP	FDP_IFC.1 (1) FMT_MSA.3
12	FDP_IFF.1 (2)	Simple security attributes (2) - UNAUTHENTICATED_APPL SFP	FDP_IFC.1 (2) FMT_MSA.3

13	FDP_IFF.1 (3)	Simple security attributes (3) - AUTHENTICATED SFP	FDP_IFC.1 (3) FMT_MSA.3
14	FDP_RIP.1	Subset residual information protection	none
15	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1
16	FPT_RVM.1	Non-bypassability of the TSP	none

Note: FPT_STM.1, FAU_STG.1, FMT_MSA.1, and FMT_SMR.1 are considered in the IT environment (see chapter 8.2.4).

5.2.1 Class FAU – Security audit

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*selection: not specified*] level of audit; and

c) [*assignment: the events specified in* Table 5.2].

FAU_GEN.1.2 - The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subjects identities, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*assignment: information specified in column four of* Table 5.2].

Table 5.2 – Auditable Events

Functional Component	Level	Auditable Event	Additional Audit Record Contents
EXT_FIA_UID.2	basic	All use of the user identification mechanism.	The user identities provided to the TOE
EXT_FIA_UAU.2	basic	All use of the user authentication mechanism.	The user identities provided to the TOE
EXT_FIA_AFL.1	minimal	The reaching of the threshold for unsuccessful authentication attempts.	The user identities provided to the TOE
FDP_IFF.1 (1)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1 (2)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1 (3)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	Detailed	Providing a timestamp	Timestamp for use in audit log files

Application Notes:

The timestamp is provided by the underlying operating system and used for logging. FPT_STM.1 is part of the environment.

The auditable event FMT_SMR.1 “Minimal: modifications to the group of users that are part of a role” is not part of the TOE (the functional component FMT_SMR.1 is part of the environment). User accounts are managed by the underlying operating system.

The auditable event FCS_COP.1 “Minimal: Success and failure, and the type of cryptographic operation” is not part of the TOE (the functional component FCS_COP.1 is part of the environment). The underlying operating system logs cryptographic operation failures.

The TOE supports two mode of operation: Normal mode and Lockdown mode. In Lockdown mode (see chapter 6.1.2.5) no logging is done since the required services are down. This is a state of exception that requires intervention by an administrator to go back to normal operation. So FAU_GEN.1 is applicable in Normal mode only.

FAU_SAR.1 Audit review

FAU_SAR.1.1	The TSF shall provide [*assignment: an authorized administrator*] with the capability to read [*assignment: all audit trail data*] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1	The TSF shall provide the ability to perform [*selection: filtering, searches, sorting*] of audit data based on: [*assignment:* *a) user identity;* *b) presumed subject address;* *c) date;* d) *time*].

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1	The TSF shall take [*assignment: alerting the administrator*] if the audit trail exceeds [*assignment: a defined capacity limit*].

5.2.2 Class FIA – Identification and authentication

Functional requirements prefixed with "EXT_"[13] are not explicitly taken from CC part 2 but rely on the functional requirements in CC part 2. These extended functional requirements have been used to avoid confusion with the "classical" identification and authentication used in CC.

EXT_FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

EXT_FIA_AFL.1.1	The TSF shall detect when [*assignment: one*] unsuccessful authentication attempts occur related to [*assignment: failed Basic authentication*]. Unlike FIA_AFL.1 (component from CC part II) the required verification of the user credentials is done outside this component and thus part of the environment.
EXT_FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*assignment: create a log file entry*].

Dependencies: EXT_FIA_UAU.2 User authentication before any action

EXT_FIA_UID.2 User identification before any action

Hierarchical to: No other components.

EXT_FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. Unlike FIA_UID.2 (component from CC part II) the required verification of the user credentials [assignment: done by local operating system or Radius server] is done outside this component and thus part of the environment.
EXT_FIA_UID.2.2	The TOE shall initiate the verification of [assignment: user data].

Dependencies: No dependencies.

[13] "EXT_" belongs to the identification; class, family and component usage is identical to the usage in CC part 2.

EXT_FIA_UAU.2 User authentication before any action

Hierarchical to: No other components.

EXT_FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Unlike FIA_UAU.2 (component from CC part II) the required verification of the user credentials [assignment: done by local operating system or Radius server] is done outside this component and thus part of the environment.

EXT_FIA_UAU.2.2 The TOE shall initiate the verification of [assignment: password data].

Dependencies: EXT_FIA_UID.2 User identification before any action.

Application note:
"other TSF-mediated actions" (EXT_FIA_UID.2 and EXT_FIA_UAU.2) means, that the user is now authorized to access the destined network resource which is defined by the firewall rules represented by FDP_IFC.1 (3) AUTHENTICATED FSP and FDP_IFF.1 (3) AUTHENTICATED FSP.

5.2.3 Class FDP – User Data Protection

FDP_IFC.1 Subset information flow control (1) – UNAUTHENTICATED SFP

FDP_IFC.1.1 The TSF shall enforce the [*assignment: UNAUTHENTICATED SFP*] on

[*assignment:*

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.

b) information: packet traffic sent through the TOE from one subject to another;

c) *operation: pass information*].

FDP_IFC.1 Subset information flow control (2) – UNAUTHENTICATED_APPL SFP

FDP_IFC.1.1 The TSF shall enforce the [*assignment: UNAUTHENTICATED_APPL SFP*] on

[*assignment:*

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.

b) information: RPC, HTTP, HTTPS, SMTP, FTP traffic sent through the TOE from one subject to another;

c) *operation: pass information*].

FDP_IFC.1 Subset information flow control (3) – AUTHENTICATED SFP

FDP_IFC.1.1 The TSF shall enforce the [*assignment: AUTHENTICATED SFP*] on

[*assignment:*

a) subjects: an external IT entity that sends and receives application level traffic information through the TOE to one another, only after the user initiating the information flow has authenticated at the TOE per EXT_FIA_UAU.2,

b) information: HTTP, HTTPS traffic sent through the TOE from one subject to another;

c) *operation: initiate service and pass information*.]

FDP_IFF.1 Simple security attributes (1) – UNAUTHENTICATED SFP

FDP_IFF.1.1 (1) The TSF shall enforce the [*assignment: UNAUTHENTICATED SFP*] based on the following types of subject and information security attributes:

[*assignment:*

a) *subject attributes:*

presumed address;

b) *information attributes:*

a. *presumed address of source subject;*

b. *presumed address of destination subject;*

c. *protocol type;*

d. *direction of connection establishment;*

e. *port numbers*].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[*assignment:*

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

a. all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

b. the presumed address of the source subject, in the information translates to an internal network address;

c. and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

a. all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

b. the presumed address of the source subject, in the information translates to an external network address;

c. *and the presumed address of the destination subject, in the information, translates to an address on the other connected network.*]

FDP_IFF.1.3 (1) The TSF shall enforce the [*assignment: none*].

FDP_IFF.1.4 (1) The TSF shall provide the following [*assignment: none*].

FDP_IFF.1.5 (1) The TSF shall explicitly authorize an information flow based on the following rules: [*assignment: none*].

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules:

[*assignment:*

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external it entity on the external network:

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network*].

FDP_IFF.1 Simple security attributes (2) – UNAUTHENTICATED_APPL SFP

FDP_IFF.1.1 (2) The TSF shall enforce the [*assignment: UNAUTHENTICATED_APPL SFP*] based on the following types of subject and information security attributes:

[*assignment:*

a) *subject attributes:*

presumed address;

b) *information attributes:*

a. *presumed address of source subject;*

b. *presumed address of destination subject;*

c. *transport layer protocol;*

d. *direction of connection establishment;*

e. *services: RPC, HTTP, HTTPS, SMTP, FTP*].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

[*assignment:*

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

a. all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

b. the presumed address of the source subject, in the information translates to an internal network address;

c. *and the presumed address of the destination subject, in the information, translates to an address on the other connected network.*

b) *Subjects on the external network can cause information to flow through the TOE to another connected network if:*

a. *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*

b. *the presumed address of the source subject, in the information translates to an external network address;*

c. *and the presumed address of the destination subject, in the information, translates to an address on the other connected network.*]

FDP_IFF.1.3 (2) The TSF shall enforce the [*assignment: none*].

FDP_IFF.1.4 (2) The TSF shall provide the following [*assignment: none*].

FDP_IFF.1.5 (2) The TSF shall explicitly authorize an information flow based on the following rules: [*assignment: none*].

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules:

[*assignment:*

a) *The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external it entity on the external network:*

c) *c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;*

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network*]

FDP_IFF.1 Simple security attributes (3) – AUTHENTICATED SFP

FDP_IFF.1.1 (3) The TSF shall enforce the [*assignment: AUTHENTICATED SFP*] based on the following types of subject and information security attributes:

[*assignment:*

a) *subject attributes:*

   a. *presumed address;*

b) *information attributes:*

   a. *user identity*

   b. *presumed address of source subject;*

   c. *presumed address of destination subject;*

   d. *protocol type;*

   e. *direction of connection establishment;*

   f. *services: HTTP, HTTPS*].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

[*assignment:*

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

   a. the human user initiating the information flow authenticates according to EXT_FIA_UAU.2;

   b. all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

   c. the presumed address of the source subject, in the information translates to an internal network address;

   d. and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

a. *the human user initiating the information flow authenticates according to EXT_FIA_UAU.2;*

b. *all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*

c. *the presumed address of the source subject, in the information translates to an external network address;*

d. *and the presumed address of the destination subject, in the information, translates to an address on the other connected network*.]

FDP_IFF.1.3 (3) The TSF shall enforce the [*assignment: none*].

FDP_IFF.1.4 (3) The TSF shall provide the following [*assignment: none*].

FDP_IFF.1.5 (3) The TSF shall explicitly authorize an information flow based on the following rules: [*assignment: none*].

FDP_IFF.1.6 (3) The TSF shall explicitly deny an information flow based on the following rules:

[*assignment:*

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external it entity on the external network:

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) *The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network*]

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*selection: allocation of the resource to*] the following objects: [*assignment: resources that are used by the subjects of the TOE to communicate through the TOE to other subjects*].

5.2.4 Class FMT – Security Management

Application Note:

The TOE does not maintain the role “authorized administrator”. Access control to the TOE is granted by the underlying operating system which also maintains the role “authorized administrator”. So FMT_SMR.1 has been placed in the environment.

FMT_MSA.3 has been chosen because of dependencies of FMT_MSA.3.1 with FDP_IFF.1. FMT_MSA.3.2 is not applicable because the TOE has unchangeable default rules (deny all).

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1	The TSF shall enforce the [*assignment: information flow UNAUTHENTICATED SFP, UNAUTHENTICATED_APPL SFP, and AUTHENTICATED SFP,*] to provide [*selection: restrictive*] default values for information flow security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow an [*assignment: authorized administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.2.5 Class FPT – Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSF is allowed to proceed.

5.2.6 Minimum strength of function

Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms. The strength of cryptographic algorithms is outside the scope of the CC. Since there is no rateable function within the TOE, there is no SOF claim.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) augmented with AVA_VLA.3 and ALC_FLR.1 (printed in bold in the table below). They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 5.3. Augmented assurance requirements have been printed in bold.

Table 5.3 – EAL4 (augmented) Assurance Requirements

Assurance Component	**Name**
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the Implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ALC_FLR.1	**Flaw remediation**
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.3	**Moderately resistant**

5.4 Functional Security Requirements for the IT Environment

This chapter defines the TOE security functional requirements for the IT environment. A list of the requirements is provided in Table 5.4. The full text of the security functional requirements is contained below.

Note: In this chapter the wording “TSF” has been changed to “IT environment” according to the CC Final Interpretation 058.

Table 5.4 – TOE Functional Security Requirements for the environment

#	Functional Requirement	Title	Dependencies
Web Identification & Authentication			
1	FIA_ATD.1	User attribute definition	none
2	FIA_UID.2	User identification before any action	none
3	FIA_UAU.2	User authentication before any action	FIA_UID.1
4	FCS_COP.1	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
Information Flow Control			
5	FMT_MSA.1 (1)	Management of security attributes (1)– UNAUTHENTICATED SFP	FDP_IFC.1 FMT_SMR.1
6	FMT_MSA.1 (2)	Management of security attributes (2) – UNAUTHENTICATED_APPL SFP	FDP_IFC.1 FMT_SMR.1
7	FMT_MSA.1 (3)	Management of security attributes (3) – AUTHENTICATED SFP	FDP_IFC.1 FMT_SMR.1
Audit			
8	FPT_STM.1	Reliable time stamps	none
9	FAU_SAR.2	Restricted audit review	FAU_SAR.1
10	FAU_STG.1	Protected audit trail storage	FAU_GEN.1
Security Management			
11	FMT_SMR.1	Security roles	FIA_UID.1

Application note:

Dependencies for FCS_COP.1 are not further resolved because these components are part of the IT environment and handled by the underlying operating system. The IT environment has to ensure that the dependencies are fulfilled. These components are listed in Table 5.5 with a corresponding explanation.

Table 5.5 – Dependencies of FCS_COP.1 fulfilled by the IT environment

FCS_CKM.1 Cryptographic key generation	The TOE has an interface to the Security Support Provider Interface (SSPI), which enables to access dynamic-link libraries containing common authentication and cryptographic data schemes. The DLLs are called Security Support Providers (SSPs). SSPs make security packages available to applications. A security package maps various SSPI functions to the security protocols specified in the package. The SSPI libraries contain functions which are used to manage and establish secure connections, like cryptographic key generation and destruction.
FCS_CKM.4 Cryptographic key destruction	
FMT_MSA.2 Secure security attributes	

All other dependencies are fulfilled by the TOE or the IT environment.

5.4.1 Class FIA – Identification and authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The IT environment shall maintain the following list of security attributes belonging to individual users: [*assignment: identity*]

Application note:

This security functional requirement is part of the environment, since the operating system or an external Radius server verifies the provided user credentials. The TOE has initiated the identification and authentication process, the environment verifies the provided user credentials and returns the result to the TOE.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The IT environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application note:

FIA_UID.2 implies that the provided user name is verified. Therefore the initiation of the verification process is represented by EXT_FIA_UID.2; the verification is represented by FIA_UID.2. This security functional requirement is part of the environment, since the operating system or an external Radius server verifies the provided user credentials.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1	The IT environment shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

FIA_UAU.2 implies that the provided password is verified. Therefore the initiation of the verification process is represented by EXT_FIA_UAU.2; the verification is represented by FIA_UAU.2. This security functional requirement is part of the environment, since the operating system or an external Radius server verifies the provided user credentials.

5.4.2 Class FCS – Cryptographic support

FCS_COP.1 Cryptographic operation

FCS_COP.1.1	The IT environment shall perform [*assignment: encryption, decryption*] in accordance with a specific cryptographic algorithm [*assignment: see Table 5.6*] and cryptographic key sizes [*assignment: see Table 5.6*] that meet the following: [*assignment: SSL protocol*]

Table 5.6 – Cipher types available in cryptographic API

Cipher type[14]	**Minimum Key length used for symmetric encryption**
SSL_RSA_WITH_RC4_128_MD5	128 Bit RC4
SSL_RSA_WITH_RC4_128_SHA	128 Bit RC4
SSL_RSA_WITH_3DES_EDE_CBC_SHA	168 Bit 3DES
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	168 Bit 3DES

Application Note:

The cryptographic API supports more cipher types, but due to A.SSL only the strong ciphers are identified.

RSA key length is set in the certificate used for the connection.

Since 1.1.2001 export regulations due to strong encryption do not longer exist, so higher encryption grades might be possible.

[14] Reference (Knowledge Base Article): http://support.microsoft.com/default.aspx?scid=kb ;en-us;245030

5.4.3 Class FPT – Protection of the TSF

FPT_STM.1 Reliable time stamps

FPT_STM.1.1	The IT environment shall be able to provide reliable time stamps.

5.4.4 Class FAU – Security audit

FAU_SAR.2 Restricted audit review

FAU_SAR.2.1	The IT environment shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1	The IT environment shall protect the storage audit records from unauthorized deletion.
FAU_STG.1.2	The IT environment shall be able to [*selection: prevent*] modifications to the audit records

5.4.5 Class FMT – Security Management

FMT_MSA.1 Management of security attributes (1) – UNAUTHENTICATED SFP

FMT_MSA.1.1 (1)	The IT environment shall enforce the [*assignment: UNAUTHENTICATED SFP*] to restrict the ability to [*assignment: add a rule, delete a rule, modify attributes in a rule,*] the security attributes [*assignment: listed in section FDP_IFF1.1 (1)*] to [*assignment: the authorized administrator*].

FMT_MSA.1 Management of security attributes (2) – UNAUTHENTICATED_APPL SFP

FMT_MSA.1.1 (2)	The IT environment shall enforce the [*assignment: UNAUTHENTICATED_APPL SFP*] to restrict the ability to [*assignment: add a rule, delete a rule, modify attributes in a rule,*] the security attributes [*assignment: listed in section FDP_IFF1.1 (2)*] to [*assignment: the authorized administrator*].

FMT_MSA.1 Management of security attributes (3) – AUTHENTICATED SFP

FMT_MSA.1.1 (3)	The IT environment shall enforce the [*assignment: AUTHENTICATED SFP*] to restrict the ability to [*assignment: add a rule, delete a rule, modify attributes in a rule,*] the security attributes [*assignment: listed in section FDP_IFF1.1 (3)*] to [*assignment: the authorized administrator*].

FMT_SMR.1 Security roles

FMT_SMR.1.1	The IT environment shall maintain the role [*assignment: authorized administrator*].
FMT_SMR.1.2	The IT environment shall be able to associate users with the role.

5.5 Security Requirements for the Non-IT Environment

No security requirements for the Non-IT environment are defined.

6 TOE Summary Specification

The TOE summary specification in the following specifies the security functionality in form of security functions as well as the assurance measures of the TOE.

6.1 TOE Security Functions

The TOE consists of three security functions (SF) which will be described in more detail in the following chapters. These security functions are:

SF1: Web Identification and Authentication

SF2: Information Flow Control

SF3: Audit

The strength of function only applies to non-cryptographic mechanisms. SF1, SF2 and SF3 do not apply to non-cryptographic, probabilistic or permutational mechanisms, so there is no SOF claim within the TOE.

6.1.1 SF1 – Web Identification and Authentication

The TOE can be configured that only particular users are allowed to access the networks through the TOE using Basic authentication (“Web publishing” rules (see 6.1.2.1 “Web publishing”) use “SF1 - Web Identification and Authentication” to authenticate users for Web access).

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. The following describes the authentication procedure: The TOE asks the client for user authentication. It gets the user name and password in clear text (base-64 encoded) and uses the data to get an impersonation token using

a) the underlying operating system (the OS verifies if the user credentials comply with the data stored in the local user database of Windows 2003 Server), or
b) a remote RADIUS server (the RADIUS Server verifies[15] if the user credentials comply with the data stored on a remote authentication server).

This token is used to pass the rules, which means the TOE decides on the basis of this logical value (yes, the user account exists; no, the user account does not exist) in combination with the other rule settings (see 6.1.2.1 “Web publishing”), if the user is allowed to access the internal resource.

[15] There is no special interface for Radius user credential verification supplied by the operating system. The TOE compiles a packet containing the user credentials, which is sent to the Radius Server and received an answer if the user can be authenticated or not.

Figure 6.1 – Web Identification & Authentication Process (local user database in OS)

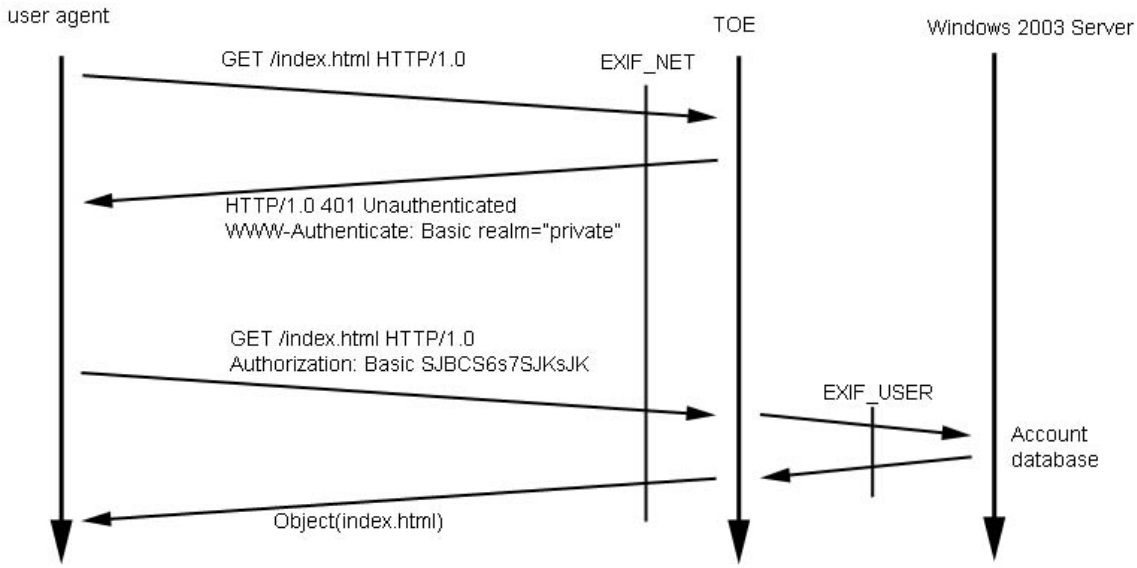
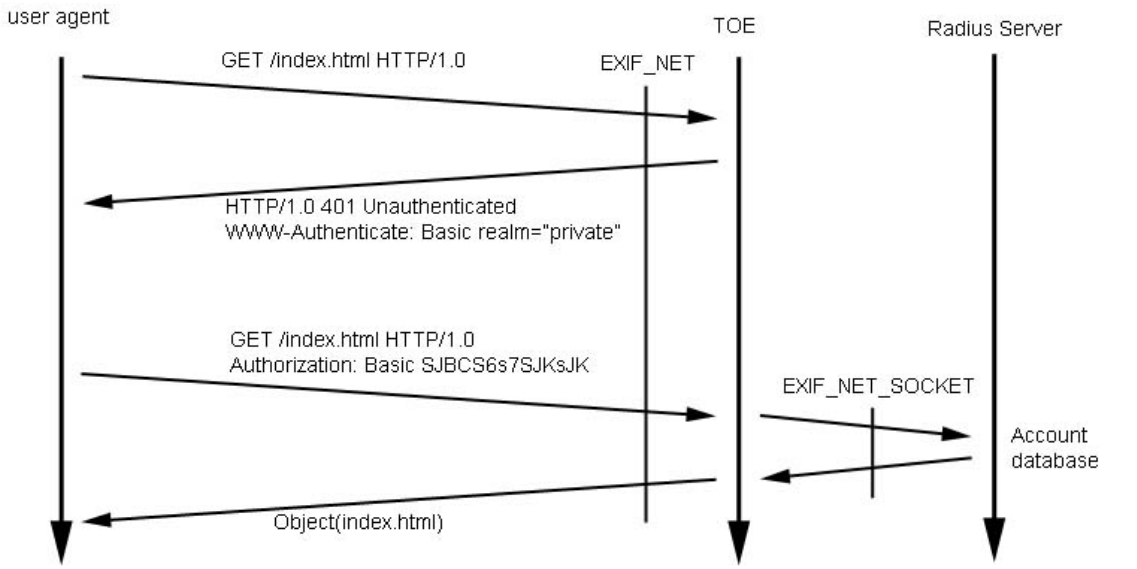


Figure 6.2 – Web Identification & Authentication Process (Radius server)



The verification of the user credentials is done in the environment. The process is initiated and finished by the TOE.

This security function has no probabilistic or permutational mechanism and therefore no SoF claim is necessary.

6.1.2 SF2 – Information Flow Control

The TOE combines several security mechanisms to enforce the security policies at different network layers: a rule base for incoming and outgoing requests, web filters and application filters, and system security configuration options.

The TOE controls the flow of incoming and outgoing 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 Firewall Policy Rules that consist of Access Rules, Network Rules, Server Publishing Rules, Mail Publishing Rules, Web Publishing Rules, and specialized Web Filters and Application Filters.

The TOE ensures that information contained in packets from previous sessions is no longer accessible once the session has been completed. The storage and processing of data packets through the TOE ensures that no residual information is transferred to future sessions through the firewall.

The TOE also supports a quota mechanism, which is used to limit the number of connections that can be established per client IP or per rule per second. This connection limit is used to protect ISA from flood and DoS attacks.

This security function has no probabilistic or permutational mechanism and therefore no SoF claim is necessary.

6.1.2.1 Firewall Policy Rules

Access rules

Define whether traffic from the source network is allowed to pass to the destination network. The TOE includes a list of preconfigured, well-known protocol definitions, including the Internet protocols which are most widely used. It is possible to add or modify additional protocols. When a client requests an object using a specific protocol, the TOE checks the access rules. A request is processed only if an access rule specifically allows the client to communicate using the specific protocol and also allows access to the requested object.

Note: It is possible to configure extended filtering for HTTP and FTP protocols. See chapter 6.1.2.2 for further details.

Network rules (route and NAT)

It is possible to configure network rules in ISA Server 2004, thereby defining and describing a network topology. Network rules determine whether there is connectivity between two networks, and what type of connectivity is defined. Networks can be connected in one of the following ways:

- Network address translation (NAT).
  When specifying this type of connection, ISA Server 2004 replaces the IP address of the client on the source network with its own IP address.
- Route.
  When specifying this type of connection, client requests from the source network are directly relayed to the destination network. The source client address is included in the request.

Routed networks are bidirectional. That is, if a routed relationship is defined from network A to network B, a routed relationship also exists from network B to network A. NAT relationships, on the other hand, are unique and unidirectional. If a NAT relationship is defined from network A to network B, no network relationship can be defined from B to A.

Server publishing & Mail publishing

The TOE uses server publishing to process incoming requests to internal servers, such as Simple Mail Transfer Protocol (SMTP) servers, FTP servers, Structured Query Language (SQL) servers, and others. Requests are forwarded downstream to an internal server, located behind the TOE.

Server publishing allows virtually any computer on your internal network to publish to the Internet. Security is not compromised because all incoming requests and outgoing responses pass through the TOE. When a server is published by the TOE, the IP addresses that are published are actually the IP addresses of the TOE. Users who request objects think that they are communicating with the TOE - whose name or IP address they specify when requesting the object - while they are actually requesting the information from the actual publishing server.

Server publishing rules determine how server publishing functions, essentially filtering all incoming and outgoing requests through the TOE. Server publishing rules map incoming requests to the appropriate servers behind the TOE. These rules will grant access dynamically, as specified, from Internet users to the specific publishing server.

Note:

A mail publishing rule defines whether requests from the destination network are allowed for mail servers on the source network. Basically this functionality is identical with Server publishing. The wizard that helps to configure the rule contains some special features to select the required protocols. The created rule (or rules when more mail protocols are required) has the same structure as a Server publishing rule.

Web publishing

The TOE uses Web publishing rules to relieve the concerns associated with publishing Web content to the Internet without compromising internal network security. Web publishing rules determine how the TOE should intercept incoming requests for HTTP objects on an internal Web server and how the TOE should respond on behalf of the Web server. Requests are forwarded downstream to an internal Web server, located behind the TOE.

Web publishing rules essentially map incoming requests to the appropriate Web servers behind the TOE.

Optionally it is possible to authenticate users, which means that a Web Publishing rule does only allow access to the network resource (e.g. a web server or web proxy) when a user provides his correct user credentials (username and password). This functionality is modeled in SF1 (see chapter 6.1.1).

Note:

By default, all incoming Web requests must go through a Web listener.

6.1.2.2 Web filters

Following extended filtering mechanism can be configured for each HTTP based protocol rule:

HTTP

The “HTTP Web filter” allows filtering of HTTP connections. It enables Header filtering, Content filtering, Method filtering and some additional checks.

OWA

The “OWA Forms-based authentication Web filter” enables forms-based (cookie) authentication for publishing Outlook Web Access servers[16].

6.1.2.3 Application filters

Application filters provide an extra layer of security at the Firewall service. Application filters can access the datastream or datagrams associated with a session within the Firewall service. Application filters are registered with the Firewall service and work with some or all application-level protocol streams or datagrams. An application filter can perform protocol-specific or system-specific tasks, such as authentication and virus checking.

[16] This is a filter which intercepts HTTP traffic. Instead of delivering the requested HTTP page, a HTTP page containing a web form is delivered. After providing the correct user credentials the requested web page is returned.

FTP access filter

The FTP filter that is provided with the TOE forwards FTP requests from SecureNAT clients to the Firewall service. The filter dynamically opens secondary ports, which are required by the FTP protocol, and performs necessary address translation for SecureNAT clients.

The FTP access filter uses the following protocol definitions, which are installed with the filter when ISA Server 2004 is installed: FTP client read only, FTP client, FTP server.

The FTP client read only mode is enforced by white list of permitted commands (not configurable).

RPC filter

The RPC filter provided with the TOE enables publishing of RPC servers, like Exchange RPC servers, making them accessible to external clients.

The RPC filter adds the “Exchange RPC (Server)” protocol definition. The RPC filter can be configured to filter specific UUIDs using the RPC Wizard within the TOE. It permits the administrator to select the services from a list of interfaces available on the server that the wizard presents, or define them manually. These service definitions can be used in server publishing rules so that external clients can access them.

SMTP filter

The Simple Mail Transfer Protocol (SMTP) filter is an application filter that intercepts all inbound SMTP traffic that arrives on port 25 of the TOE.

The SMTP filter can also be configured to accept or deny certain SMTP commands and to accept only a specified command length.

6.1.2.4 System policy

ISA Server 2004 protects network resources, while connecting them securely for specifically defined needs. ISA Server introduces a system policy, a set of firewall policy rules that control how the ISA Server computer enables the infrastructure necessary to manage network security and connectivity. ISA Server is installed with a default system policy, designed to address the balance between security and connectivity.

Some system policy rules are enabled upon installation. These are considered the most basic and necessary rules for effectively managing the ISA Server 2004 environment. You can subsequently identify those services and tasks that you require to manage your network, and enable the appropriate system policy rules.

When the Firewall Service is down, the Firewall driver goes into the so called “Lockdown” mode. Only lockdown policy rules traffic is allowed in this mode. This is done in order to permit administrators to troubleshoot the machine from remote[17].

[17] Remote administration is not part of evaluation.

6.1.2.5 Lockdown Mode

The TOE's lockdown feature combines the need for isolation with the need to stay connected. Whenever a situation occurs that causes the Firewall service to shut down, the TOE enters the lockdown mode. When the TOE is in lockdown mode, a restricted set of system policy rules are always applicable (all of the corresponding functionalities are handled by the environment (the operating system the TOE is installed on) and not by the TOE itself[18]).

Also outgoing traffic from the Local Host network to all networks is allowed. If an outgoing connection is established, that connection can be used to respond to incoming traffic. For example, a DNS query can receive a DNS response, on the same connection.

No incoming traffic is allowed, unless a system policy rule (see chapter 6.1.2.4) that specifically allows the traffic is enabled (by default system policy rules define traffic from and to the local host only).

Rules processed in Lockdown Mode are handled with FDP_IFC.1 (1) UNAUTHENTICATED FSP, FDP_IFC.1 (2) UNAUTHENTICATED_APPL SFP, FDP_IFC.1 (3) AUTHENTICATED FSP, FDP_IFF.1 (1) UNAUTHENTICATED FSP, FDP_IFF.1 (2) UNAUTHENTICATED_APPL SFP, and FDP_IFF.1 (3) AUTHENTICATED FSP, since the same functionality (and code) is invoked when the Lockdown Mode is entered.

In Lockdown mode no logging is done since the required services are down. This is a state of exception that requires intervention by an administrator to go back to normal operation. This is considered in the scope of FAU_GEN.1 in the Application Note.

6.1.3 SF3 – Audit

The TOE stores logging information in different log files in the environment:

- Firewall service log

  The Firewall log contains records of packets that were dropped in the packet filter level. It is possible to turn on logging for packets that were permitted to traverse the firewall. Access Rules can be configured selectively to create or not to create a log file entry when a packet has been blocked or permitted.

- Web proxy service log

  The Web Proxy log stores a line per HTTP request that it gets. Each request (incoming and outgoing) is always logged.

- Windows application event log

[18] For example: There is a System Policy Rules with allows NetBIOS traffic from the localhost to internal clients. NetBIOS is a functionality which is handled by Windows Operating System and explicitly allowed by the System Policy Rule.

The Windows application event log stores important system events and failures. and detects the occurrence of the following selected events:

- access rules permitted (firewall service log),
- access rules denied (firewall service log),
- failed authentication of users (firewall service log),
- passed requests though the TOE (firewall service log),
- passed requests of users that have been previously authenticated through the TOE (firewall service log),
- received (incoming and outgoing) HTTP requests (web proxy log),
- log failure (windows event log),
- service started, stopped or not responding (windows event log).

The log files can be audited[19] using a component called Logviewer inside the MMC.

Note 1:

In Lockdown mode (see chapter 6.1.2.4) no logging is done since the required services are down. This is a state of exception that requires intervention by an administrator to go back to normal operation.

Note 2:

The Web Proxy and Firewall logs can include a result code field that specifies the status of the request. This field can be used to indicate Windows (Win32) error code, HTTP status code, or Winsock error codes.

This security function has no probabilistic or permutational mechanism and therefore no SoF claim is necessary.

[19] This includes several sorting and filtering features.

6.1.4 Assignment of SFs to security functional requirements

The justification of the mapping between security functional requirements and security functions is given in this chapter 6.1.4. The results are summarized in Table 6.1.

Table 6.1 – Assignment of security functional requirements to security functions

#	SFR	SF1	SF2	SF3
1	FAU_GEN.1			X
2	FAU_SAR.1			X
3	FAU_SAR.3			X
4	FAU_STG.3			X
5	EXT_FIA_AFL.1	X		
6	EXT_FIA_UID.2	X		
7	EXT_FIA_UAU.2	X		
8	FDP_IFC.1 (1) – UNAUTHENTICATED SFP		X	
9	FDP_IFC.1 (2) – UNAUTHENTICATED_APPL SFP		X	
10	FDP_IFC.1 (3) – AUTHENTICATED SFP		X	
11	FDP_IFF.1 (1) – UNAUTHENTICATED SFP		X	
12	FDP_IFF.1 (2) – UNAUTHENTICATED_APPL SFP		X	
13	FDP_IFF.1 (3) – AUTHENTICATED SFP		X	
14	FDP_RIP.1		X	
15	FMT_MSA.3		X	
16	FPT_RVM.1		X	

FAU_GEN.1 (Audit data generation) is mapped to SF3 and outlines what data must be included in audit records. Audit data generated by the TOE is stored in different log files as stated in SF3. When applicable, information about the identified user is stored in the log files.

This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN because the TOE generates a readable audit trail of security-related events which contains user accountability for information flows.

FAU_SAR.1 (Audit review) is mapped to SF3 and ensures that the user can interpret the recorded information. The log data is

a. stored in a human readable form in a database by the TOE and can be reviewed by the Logviewer component that runs inside the MMC, or

b. special events are stored in the Windows Event Log which can be reviewed with the Event Viewer (which is part of the operating system).

This component traces back to and aids in meeting the following objective: O.AUDREC because the TOE generates a human readable (clear text) audit trail of security-related events.

FAU_SAR.3 (Selectable Audit review) is mapped to SF3 and ensures that a variety of filtering, searching and sorting can be performed on the audit trail.

This component traces back to and aids in meeting the following objective: O.AUDREC because the TOE supports filter, search and sort facilities on the audit trail.

FAU_STG.3 (Action in case of possible audit data loss) is mapped to SF3 and ensures that the user is alerted in case of possible audit data loss.

This component traces back to and aids in meeting the following objective: O.AUDREC because the TOE makes sure that no records are lost (for example of not enough storage capacity).

EXT_FIA_AFL.1 (Authentication failure handling) is mapped to SF1. This component exists to specify action after some number of unsuccessful authentication attempts. It ensures that users cannot endlessly attempt to authenticate without leaving no trace in the log files.

This component traces back to and aids in meeting the following objectives: O.IDAUTH because the TOE uniquely identifies the user and authenticates the claimed identify for all users.

EXT_FIA_UID.2 (User identification before any action) is mapped to SF1. This component ensures that the user identify himself (when required) before any information is passed though the TOE. The Basic authentication method provides this functionality for the users.

This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN because the user is identified with his username witch has to exist in the local user database to be authenticated successfully.

EXT_FIA_UAU.2 (User authentication before any action) is mapped to SF1 and ensures that users are identified when necessary. When authentication is required it must occur before any data is passed though the TOE. Basic authentication method provides this functionality for the users. Note, that firewall administrators are not authenticated by the TOE itself. This is done by the environment (underlying operating system).

This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN because the user is identified with his username witch has to exist in the local user database to be authenticated successfully.

Application Note:

This Security Target consists of multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP_IFC.1 for each of the three named information flow control policies. Following SFPs exist:

- UNAUTHENTICATED SFP and UNAUTHENTICATED_APPL SFP

  The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities.

- AUTHENTICATED SFP

  The subjects under control of this policy are human users on an internal or external network who must be authenticated at the TOE before using the services in EXT_FIA_UAU.2. The information flowing between subjects in both policies is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. The rules that define each information flow control SFP are found in FDP_IFF.1.2. Component FDP_IFF.1 is iterated third times to correspond to each of the three iterations of FDP_IFC.1.

FDP_IFC.1 (1) (Subset information flow control (1)) is mapped to SF2 and identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). It refers to the IP packet filters and Server publishing mentioned in SF2.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_IFC.1 (2) (Subset information flow control (2)) is mapped to SF2 and identifies the entities involved in the UNAUTHENTICATED_APPL information flow control SFP (i.e., users sending information on application level to other users and vice versa). It refers to the Access rules, Web publishing rules, and Server publishing rules that are used unauthenticated mentioned in SF2.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_IFC.1 (3) (Subset information flow control (3)) is mapped to SF2 and identifies the entities involved in the AUTHENTICATED information flow control SFP. Users who want to use one of these services must be authenticated at the TOE. It refers to the HTTP and

HTTPS protocols used in Access rules, Web publishing rules, and Server publishing rules that are used authenticated as mentioned in SF2.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_IFF.1 (1) (Simple security attributes (1)) is mapped to SF2 (Access Rules, Network Rules, System Policy) and identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_IFF.1 (2) (Simple security attributes (2)) is mapped to SF2 (Network Rules, Server publishing, Web publishing, HTTP, FTP access filter[20], SMTP filter) and identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED_APPL SFP for data transferred on application level, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_IFF.1 (3) (Simple security attributes (3)) is mapped to SF2 (Network Rules, Server publishing, Web publishing, HTTP, OWA, FTP access filter, RPC filter) and identifies the attributes of the users sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information (data sent on application level) is permitted to flow.

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FDP_RIP.1 (Subset residual information protection) is mapped to SF2 and ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. Future sessions will not contain residual information of previous sessions in padding data.

[20] Anonymous FTP

This component traces back to and aids in meeting the following objective: O.MEDIAT because the TOE mediates the flow of all information from users on a connected network to users on another connected network.

FMT_MSA.3 (Static attribute initialization) is mapped to SF2. This component ensures that there is a default deny policy for the information flow control security rules. The TOE ensures that by default all traffic through the TOE is denied.

This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA because the TOE mediates the flow of all information from users on a connected network to users on another connected network and ensures that the TOE must not compromises its resources or those of any connected network.

FPT_RVM.1 (Non-bypassability of the TSP) is mapped to SF2 and ensures that on initial start-up of the TOE or recovery from an interruption the security function is invoked before any information is transmitted via the TOE.

This component traces back to and aids in meeting the following objective: O.SECSTA because it ensures that the TOE must not compromises its resources or those of any connected network on initial start-up or recovery from an interruption.

6.2 Assurance Measures

In Table 6.2 the TOE specific assurance measures are listed (augmented assurance requirements have been printed in bold). These measures, mainly consisting of providing appropriate documentation, are fulfilling the requirements from table 5.2:

Table 6.2 – Assurance requirements and assurance measures

Assurance requirements according to EAL4	Assurance measures of the developer
Configuration management ACM_AUT.1 (Partial CM automation) ACM_CAP.4 (Generation support and acceptance procedures) ACM_SCP.2 (Problem tracking CM coverage)	Application of a QM System including configuration control, generation support and acceptance procedures, and problem tracking CM coverage.
Delivery and operation ADO_DEL.2 (Detection of modification) ADO_IGS.1 (Installation, generation and start-up procedures)	Documentation of the TOE's protection mechanisms with regard to delivery, installation and start-up.

Development ADV_FSP.2 (Fully defined external interfaces) ADV_HLD.2 (Security enforcing high-level design) ADV_IMP.1 (Subset of the Implementation of the TSF) ADV_LLD.1 (Descriptive low-level design) ADV_RCR.1 (Informal correspondence demonstration) ADV_SPM.1 (Informal TOE security policy model)	Definition of CC requirements with regard to development procedures and documentation, high-level and low-level design, functional specification and corresponding demonstration, implementation (source code), and a informal TOE security policy model.
Guidance documents AGD_ADM.1 (Administrator guidance) AGD_USR.1 (User guidance)	Creating and delivery of administrator and user guidance.
Life cycle support ALC_DVS.1 (Identification of security measures) ALC_LCD.1 (Developer defined life-cycle model) ALC_TAT.1 (Well-defined development tools) **ALC_FLR.1 (Flaw remediation)**	Defines requirements for assurance through the adoption of a well defined life-cycle model for all the steps of the TOE development, including the identification of security measures and the well-defined development tools. Description how security flaws are tracked and corrected by the developer.
Tests ATE_COV.2 (Analysis of coverage) ATE_DPT.1 (Testing: high-level design) ATE_FUN.1 (Functional testing) ATE_IND.2 (Independent testing – sample)[21]	Testing of the TSF, whether the TOE behaves as specific in the design documentation and in accordance with the TOE security functional environment. This also includes a depth and covering analysis. ATE_IND.2 (Independent testing) testing is done by the evaluation body.
Vulnerability assessment AVA_MSU.2 (Validation of analysis) AVA_SOF.1 (Strength of TOE security function evaluation) **AVA_VLA.3 (Moderately resistant)**	Analyzing the vulnerability analysis of obvious TOE vulnerabilities (VLA document). Also a misuse analysis is provided. SOF analysis is not required (no claim).

[21] Not developer relevant, since tests are done by the evaluation body.

7 PP Claims

This security target does not claim for compliance with any existing protection profile.

Some aspects are leant on the

- “Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, U.S. Government of Defense, June 22, 2000” [PP1], and
- “Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, U.S. Government of Defense, April 1999” [PP2].

8 Rationale

This chapter provides the evidence used in the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements.

8.1 Security Objectives Rationale

Table 8.1 maps assumptions and threats to objectives, demonstrating that all assumptions and threats are mapped to at least one objective. Table 8.2 maps objectives to threats and assumptions, demonstrating that all objectives are mapped to at least one threat or assumption. A discussion of the rationale for threat mappings is provided below.

Table 8.1 – Mapping the TOE Security Environment to Objectives

#	**Assumption / Threat / OSP**	**Security Objective**
1	A.PHYSEC	OE.PHYSEC
2	A.GENPUR	OE.GENPUR
3	A.NOEVIL	OE.NOEVIL
4	A.SINGEN	OE.SINGEN
5	A.DIRECT	OE.DIRECT
6	A.SECINST	OE.SECINST
7	A.ENV	OE.ENV
8	A.WEBI&A	OE.WEBI&A
9	A.SSL	OE.SSL
10	T.NOAUTH	O.IDAUTH, O.SECSTA
11	T.MEDIAT	O.MEDIAT
12	T.OLDINF	O.MEDIAT
13	T.AUDFUL	O.AUDREC
14	P.AUDACC	O.AUDREC, O.ACCOUN

Table 8.2 – Tracing of Security Objectives to Threats, OSPs and Assumptions

#	Security Objective	Threat / Assumption / OSP
1	OE.PHYSEC	A.PHYSEC
2	OE.GENPUR	A.GENPUR
3	OE.NOEVIL	A.NOEVIL
4	OE.SINGEN	A.SINGEN
5	OE.DIRECT	A.DIRECT
6	OE.SECINST	A.SECINST
7	OE.ENV	A.ENV
8	OE.WEBI&A	A.WEBI&A
9	OE.SSL	A.SSL
10	O.IDAUTH	T.NOAUTH
11	O.MEDIAT	T.MEDIAT, T.OLDINF
12	O.SECSTA	T.NOAUTH
13	O.AUDREC	P.AUDACC, T.AUDFUL
14	O.ACCOUN	P.AUDACC

Note:

The security objectives for the environment are a restatement of the assumptions for the environment.

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.NOAUTH is countered by O.IDAUTH, O.SECSTA because the security objective ensures that the user has to authenticate before access is granted to TOE functions and the TOE ensures that it does not compromise its resources or those of any connected network.

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.MEDIAT is countered by O.MEDIAT because the security objective ensures that the TOE mediates the flow of all information from users on the connected network to users on another connected network.

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 data of the information flows from the TOE. Padding data ensures that data packets contain the required number of bits and bytes and could contain residual information from previous connections.”

T.OLDINF is countered by O.MEDIAT because the security objective ensures that the TOE mediates the flow of all information from users on the connected network to users on another connected network and ensures that information from a previous information flow is not available.

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.”

T.AUDFUL is countered by O.AUDREC because the security objective ensures that the TOE records a reliable readable audit trail and that no records are left because of less storage capacity.

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."

P.AUDACC is countered by O.AUDREC, O.ACCOUN because the security objective ensures that a person is identified to make the person accountable for the action and that this action is logged in the audit trail.

O.IDAUTH: This security objective is necessary to counter the threat T.NOAUTH. It requires that users be uniquely identified before accessing the TOE and sending information through the TOE.

O.MEDIAT: This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.SECSTA: Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network and thus counters the threats: T.NOAUTH.

O.AUDREC: This security objective is necessary to counter the policy: P.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in

the audit trail and T.AUDFUL by requiring that no records are left because of not enough storage capacity.

O.ACCOUN: This security objective is necessary to counter the policy: P.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

8.2 Security Requirements Rationale

In this chapter, the security objectives are mapped to the functional requirements and the rationale is provided for the selected EAL and its components and augmentation.

8.2.1 Security Functional Requirements Rationale

The mapping of security objectives to functional requirements (components) is provided in Table 8.3. The mapping of security objectives of the environment to functional requirements (components) is provided in Table 8.5.

Table 8.3 – Security Objective to Functional Component Mapping

#	Security Objectives	Functional Component (SFR TOE)
1	O.IDAUTH	EXT_FIA_AFL.1, EXT_FIA_UID.2, EXT_FIA_UAU.2
2	O.MEDIAT	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_IFF.1 (3), FMT_MSA.3, FDP_RIP.1
3	O.SECSTA	FMT_MSA.3, FPT_RVM.1
4	O.AUDREC	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.3
5	O.ACCOUN	FAU_GEN.1, EXT_FIA_UID.2, EXT_FIA_UAU.2

Table 8.4 – Functional Requirements to Objectives Mapping

#	Functional Requirements (SFR TOE)	Security Objectives
1	FAU_GEN.1	O.AUDREC, O.ACCOUN
2	FAU_SAR.1	O.AUDREC
3	FAU_SAR.3	O.AUDREC
4	FAU_STG.3	O.AUDREC
5	EXT_FIA_AFL.1	O.IDAUTH
6	EXT_FIA_UID.2	O.IDAUTH, O.ACCOUN

7	EXT_FIA_UAU.2	O.IDAUTH, O.ACCOUN
8	FDP_IFC.1 (1)	O.MEDIAT
9	FDP_IFC.1 (2)	O.MEDIAT
10	FDP_IFC.1 (3)	O.MEDIAT
11	FDP_IFF.1 (1)	O.MEDIAT
12	FDP_IFF.1 (2)	O.MEDIAT
13	FDP_IFF.1 (3)	O.MEDIAT
14	FMT_MSA.3	O.MEDIAT, O.SECSTA
15	FDP_RIP.1	O.MEDIAT
16	FPT_RVM.1	O.SECSTA

A discussion of the rationale for the mapping is provided for each security objective below.

O.IDAUTH: The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

O.IDAUTH is mapped to EXT_FIA_AFL.1, EXT_FIA_UID.2, EXT_FIA_UAU.2.

- EXT_FIA_AFL.1 Authentication failure handling

  This component exists to specify action after some number of unsuccessful authentication attempts. It ensures that users cannot endlessly attempt to authenticate without leaving no trace in the log files.

- EXT_FIA_UID.2 User identification before any action

  This component ensures that the user identify himself (when required) before any information is passed though the TOE. The Basic authentication method provides this functionality for the users.

- EXT_FIA_UAU.2 User authentication before any action

  This component ensures that users are identified when necessary. When authentication is required it must occur before any data is passed though the TOE. Basic authentication method provides this functionality for the users. Note, that firewall administrators are not authenticated by the TOE itself. This is done by the environment (underlying operating system).

O.MEDIAT: The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

O.MEDIAT is mapped to FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_IFF.1 (3), FMT_MSA.3, FDP_RIP.1.

- FDP_IFC.1 Subset information flow control (1)

  This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa).

- FDP_IFC.1 Subset information flow control (2)

  This component identifies the entities involved in the UNAUTHENTICATED_APPL information flow control SFP (i.e., users sending information on application level to other users and vice versa).

- FDP_IFC.1 Subset information flow control (3)

  This component identifies the entities involved in the AUTHENTICATED information flow control SFP. Users who want to use one of these services must be authenticated at the TOE.

- FDP_IFF.1 Simple security attributes (1)

  This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.

- FDP_IFF.1 Simple security attributes (2)

  This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICATED_APPL SFP for data transferred on application level, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow.

- FDP_IFF.1 Simple security attributes (3)

  This component identifies the attributes of the users sending and receiving the information in the AUTHENTICATED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information (data sent on application level) is permitted to flow.

- FMT_MSA.3 Static attribute initialization

  This component ensures that there is a default deny policy for the information flow control security rules. The TOE ensures that by default all traffic through the TOE is denied.

- FDP_RIP.1 Subset residual information protection

  This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. Future sessions will not contain residual information of previous sessions in padding data.

O.SECSTA: Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.SECSTA is mapped to FMT_MSA.3 and FPT_RVM.1.

- FMT_MSA.3 Static attribute initialization

  This component ensures that there is a default deny policy for the information flow control security rules. The TOE ensures that by default all traffic through the TOE is denied.

- FPT_RVM.1 Non-bypassability of the TSP

  This component ensures that upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE security function is invoked before any information can be transmitted through the TOE.

O.AUDREC: The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. The TOE must provide that the audit trail is readable and no records are left because of not enough storage capacity.

O.AUDREC is mapped to FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, and FAU_STG.3.

- FAU_GEN.1 Audit data generation

  This component outlines what data must be included in audit records. Audit data generated by the TOE is stored in different log files as stated in SF3. When applicable, information about the identified user is stored in the log files.

- FAU_SAR.1 Audit review

  This component ensures that the user can interpret the recorded information. The log data is

  a) stored in a human readable form in a database by the TOE and can be reviewed by the Logviewer component that runs inside the MMC, or

  b) special events are stored in the Windows Event Log which can be reviewed with the Event Viewer (which is part of the operating system).

- FAU_SAR.3 Selectable Audit Review

  This component ensures that a variety of filtering, searching and sorting can be performed on the audit trail.

- FAU_STG.3 Action in case of possible audit data loss

  This component ensures that the user is alerted in case of possible audit data loss.

O.ACCOUN: The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

O.ACCOUN is mapped to FAU_GEN.1, EXT_FIA_UID.2, EXT_FIA_UAU.2.

- FAU_GEN.1 Audit data generation

  This component outlines what data must be included in audit records. Audit data generated by the TOE is stored in different log files as stated in SF3. When applicable, information about the identified user is stored in the log files.

- EXT_FIA_UID.2 User identification before any action

  This component ensures that the user identify himself (when required) before any information is passed though the TOE. The Basic authentication method provides this functionality for the users.

- EXT_FIA_UAU.2 User authentication before any action

  This component ensures that users are identified when necessary. When authentication is required it must occur before any data is passed though the TOE. Basic authentication method provides this functionality for the users. Note, that firewall administrators are not authenticated by the TOE itself. This is done by the environment (underlying operating system).

Table 8.5 – Security Objective to Functional Component of the IT environment Mapping

#	Objective (IT Environment)	Functional Component
1	OE.ENV	FPT_STM.1, FAU_SAR.2, FAU_STG.1, FMT_SMR.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FCS_COP.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2
2	OE.WEBI&A	FIA_ATD.1, FIA_UAU.2, FIA_UID.2

Table 8.6 – Functional Requirements to Objectives for the IT environment Mapping

#	Functional Requirement	Objective
1	FPT_STM.1	OE.ENV
2	FAU_SAR.2	OE.ENV
3	FAU_STG.1	OE.ENV
4	FMT_SMR.1	OE.ENV
5	FMT_MSA.1 (1) – UNAUTHENTICATED SFP	OE.ENV
6	FMT_MSA.1 (2) – UNAUTHENTICATED_APPL SFP	OE.ENV
7	FMT_MSA.1 (3) – AUTHENTICATED SFP	OE.ENV
8	FCS_COP.1	OE.ENV
9	FIA_ATD.1	OE.ENV, OE.WEBI&A
10	FIA_UAU.2	OE.ENV, OE.WEBI&A

11	FIA_UID.2	OE.ENV, OE.WEBI&A

A discussion of the rationale for the mapping is provided for each objective below.

OE.WEBI&A: When a Radius Server is used for web identification & authentication, it has to be placed on the internal network, so that data transferred to and from the Radius Server is secured by the TOE from external entities.

OE.WEBI&A is mapped to FIA_ATD.1, FIA_UAU.2, FIA_UID.2

- FIA_ATD.1 User attribute definition
  This component ensures that the user credentials which are provided to the TOE are verified by either the operating system (local user database) or a Radius Server (refers to the Radius Server only; see OE.ENV for local user database). OE.WEBI&A ensures that the required Radius Server is placed on the internal network.
- FIA_UID.2 User identification before any action
  This component ensures that the provided user credentials (the username) are verified by the IT environment (refers to the Radius Server only; see OE.ENV for local user database).
- FIA_UAU.2 User authentication before any action
  This component ensures that the provided user credentials (the password) are verified by the IT environment (refers to the Radius Server only; see OE.ENV for local user database).

OE.ENV: The OS has to implement functions for: reliable time stamp, file protection, tools for audit review, and verification of user credentials that can be used by the TOE.

OE.ENV is mapped to FPT_STM.1, FAU_SAR.2, FAU_STG.1, FMT_SMR.1, FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FCS_COP.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2.

- FPT_STM.1 Reliable time stamps

  This component ensures that the date and time on the TOE is dependable. This is important for the audit trail to trace recorded audit data.
- FAU_SAR.2 Restricted audit review

  This component ensures that audit log files can be reviewed by authorized persons only. The operating system restricts access to protected log files to authorized persons.
- FAU_STG.1 Protected audit trail storage

  This component ensures that the audit data cannot be deleted by unauthorized persons. The operating system restricts access to protected log files to authorized persons.

- FMT_SMR.1 Security roles

  Each of the CC class FMT components in this Security Target depend on this component. It requires the ST writer to choose roles. The role “authorized administrator” is defined by this component and ensures that the underlying operating system is responsible for implementing such role.

- FMT_MSA.1 Management of security attributes (1) – UNAUTHENTICATED SFP

  This component ensures the TSF enforces the UNAUTHENTICATED SFP to restrict the ability to change specified security attributes that are listed in section FDP_IFF1.1 (1).

- FMT_MSA.1 Management of security attributes (2) – UNAUTHENTICATED_APPL SFP

  This component ensures the TSF enforces the UNAUTHENTICATED_APPL SFP to restrict the ability to change specified security attributes that are listed in FDP_IFF1.1 (2).

- FMT_MSA.1 Management of security attributes – AUTHENTICATED SFP

  This component ensures the TSF enforces the AUTHENTICATED SFP to restrict the ability to change specified security attributes that are listed in section FDP_IFF1.1 (3).

- FCS_COP.1 Cryptographic operation

  This component ensures that SSL encryption can be used for

  - securing a Basic authentication and
  - establishing an SSL bridging connection.

- FIA_ATD.1 User attribute definition
  This component ensures that the user credentials which are provided to the TOE are verified by either the operating system (local user database) or a Radius Server (refers to the local user database provided by the operating system only; see OE.WEBI&A for Radius Server).

- FIA_UID.2 User identification before any action
  This component ensures that the provided user credentials (the username) are verified by the IT environment (refers to the local user database provided by the operating system only; see OE.WEBI&A for Radius Server).

- FIA_UAU.2 User authentication before any action
  This component ensures that the provided user credentials (the password) are verified by the IT environment (refers to the local user database provided by the operating system only; see OE.WEBI&A for Radius Server).

8.2.2 Security Assurance Requirements Rationale

EAL4 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behavior. The augmentation with AVA_VLA.3 provides resistance against attackers with moderate attack potential and ensures that the evidence shows that the search for vulnerabilities is systematic; the augmentation with ALC_FLR.1 ensures that the developer has documented a flaw remediation procedure, that describe the procedures used to track all reported security flaws, the status of finding a correction of the flaw and the methods used to provide flaw information, corrections and guidance on corrective actions. Assurance is additionally gained through an informal model of the TOE security policy. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a medium attack potential.

Beside this general description, the TOE itself acts as secure gateway with a basic up to medium level of protection. Thereby different operation scenarios are linked to different levels of needed protection.

Therefore the TOE shall suffice an adequate security level for the processing information and a complying level of assurance. The chosen assurance level EAL4 (augmented with ALC_FLR.1 and AVA_VLA.3) offer a complying level of assurance.

8.2.3 Strength of Function Rationale

The strength of function only applies to non-cryptographic mechanisms. SF1, SF2 and SF3 do not apply to non-cryptographic, probabilistic or permutational mechanisms, so there is no SOF claim within the TOE.

8.2.4 Dependency Rationale

Table 8.7 – TOE Functional Requirements Dependencies

#	Requirement (SFR TOE)	Dependencies
1	FAU_GEN.1	FPT_STM.1
2	FAU_SAR.1	FAU_GEN.1
3	FAU_SAR.3	FAU_SAR.1
4	FAU_STG.3	FAU_STG.1

5	EXT_FIA_AFL.1	EXT_FIA_UAU.2
6	EXT_FIA_UID.2	none
7	EXT_FIA_UAU.2	EXT_FIA_UID.2
8	FDP_IFC.1 (1) – UNAUTHENTICATED SFP	FDP_IFF.1 (1)
9	FDP_IFC.1 (2) – UNAUTHENTICATED_APPL SFP	FDP_IFF.1 (2)
10	FDP_IFC.1 (3) – AUTHENTICATED SFP	FDP_IFF.1 (3)
11	FDP_IFF.1 (1) – UNAUTHENTICATED SFP	FDP_IFC.1 (1), FMT_MSA.3
12	FDP_IFF.1 (2) – UNAUTHENTICATED_APPL SFP	FDP_IFC.1 (2), FMT_MSA.3
13	FDP_IFF.1 (3) – AUTHENTICATED SFP	FDP_IFC.1 (3), FMT_MSA.3
14	FDP_RIP.1	none
15	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
16	FPT_RVM.1	none

Table 8.8 – Functional Requirements Dependencies for the IT Environment

#	**Requirement (SFR Environment)**	**Dependencies**
1	FIA_ATD.1	none
2	FIA_UID.2	none
3	FIA_UAU.2	FIA_UID.1 (covered by FIA_UID.2)
4	FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
5	FMT_MSA.1 (1)	FDP_IFC.1 (1), FMT_SMR.1
6	FMT_MSA.1 (2)	FDP_IFC.1 (2), FMT_SMR.1
7	FMT_MSA.1 (3)	FDP_IFC.1 (3), FMT_SMR.1
8	FPT_STM.1	none
9	FAU_SAR.2	FAU_SAR.1
10	FAU_STG.1	FAU_GEN.1
11	FMT_SMR.1	FIA_UID.1

FIA_ATD.1, FIA_UAU.2 and FIA_UID.2 are part of the environment, since the operating system or an external Radius server verify the provided user credentials.

The timestamp is provided by the underlying operating system. So FPT_STM.1 is part of the IT environment.

The TOE does not maintain the role “authorized administrator”. Access control to the TOE is granted by the underlying operating system that also maintains the role “authorized administrator”. So FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), and FMT_SMR.1 have been placed in the IT environment.

Access to the log files is restricted to authorized persons by the underlying operating system, so FAU_STG.1 and FAU_SAR.2 have been placed in the IT environment.

Cryptographic support is part of the underlying operating system that provides

- the Crypto API (CAPI) for common cryptographic operations and
- Schannel.dll for SSL related operations.

Dependencies for FCS_COP.1 are not further resolved because these components are part of the environment and handled by the underlying operating system. The IT environment has to ensure that the dependencies are fulfilled. These components are listed in Table 8.9 with a corresponding explanation.

Table 8.9 – Dependencies of FCS_COP.1 fulfilled by the IT environment

FCS_CKM.1 Cryptographic key generation	The TOE has an interface to the Security Support Provider Interface (SSPI), which enables to access dynamic-link libraries containing common authentication and cryptographic data schemes. The DLLs are called Security Support Providers (SSPs). SSPs make security packages available to applications. A security package maps various SSPI functions to the security protocols specified in the package. The SSPI libraries contain functions which are used to manage and establish secure connections, like cryptographic key generation and destruction.
FCS_CKM.4 Cryptographic key destruction	
FMT_MSA.2 Secure security attributes	

8.3 TOE Summary Specification Rationale

This chapter shows that the TOE security functions and assurance measures are suitable to meet the TOE Security Requirements.

8.3.1 TOE Security Functions Rationale

Table 6.1 in chapter 6 shows that the security functions defined in the TOE Summary Specification address all of the TOE security functional requirements. All security functions are necessary because there is at least one security functional requirement mapped to each security function. The corresponding rationale and the mapping is provided for each security functional requirement within chapter 6.1.

8.3.2 Security Requirements are mutually supportive and internally consistent

All security functional requirements are taken from the Common Criteria part 2, except the functional requirements prefixed with “EXT_”, which are not explicitly taken from CC part 2 but which rely on the functional requirements in CC part 2. These extended functional requirements have been used to avoid confusion with the “classical” identification and

authentication used in CC. The TOE - together with its environment - fulfils all the dependencies defined in the selected SFRs. This shows that the security functions work together so as to satisfy the security functional requirements.

The Table 6.1 shows that all security functional requirements are satisfied by at least one security function. The definitions of the security functional requirements and the assurance components in the preceding chapters demonstrate that mutual support and consistency are given for both groups of requirements. The fact that the SFRs and the assurance requirements support each other and that there are no inconsistencies between these groups is shown in the chapters above.

8.3.3 Assurance Measures Rationale

The Table 6.2 in chapter 6 shows how all assurance requirements were satisfied and that there is at least one assurance measure defined in the TOE Summary Specification to meet each of the security assurance requirements.

8.4 PP Claims Rationale

This security target is in no compliance with any existing protection profile.

9 Appendix

9.1 References

[CC] *Common Criteria for Information Technology Security Evaluation*, version 2.1, revision August 1999, *Incorporated with interpretations as of 2003-12-31*
Part 1: Introduction and general model, CCIMB-99-031,
Part 2: Security functional requirements, CCIMB-99-032,
Part 3: Security Assurance Requirements, CCIMB-99-033

[CEM] *Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and general model*, version 0.6, revision 11.01.1997, *Part 2: Evaluation Methodology,* version 1.0, revision August 1999
Incorporated with interpretations as of 2003-12-31

[MSISA] *Microsoft Internet Security and Acceleration Server 2004 EE manual – Enterprise Edition,* Microsoft Corp.

[RADIUS] RFC 2865 - Remote Authentication Dial In User Service (RADIUS), http://www.faqs.org/rfcs/rfc2865.html

[PP1] *Application-level Firewall Protection Profile for Basic Robustness Environments*, Version 1.0, U.S. Government of Defense, June 22, 2000

[PP2] *Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, U.S. Government of Defense, April 1999"

[WINST] Microsoft Windows 2003/XP Security Target, Version 1.0. 28.09.2005, Microsoft Corporation

[WINVR] National Information Assurance Partnership, Common Criteria Evaluation and Validation Scheme Validation Report Microsoft Windows 2003 Server and XP Workstation Report Number: CCEVS-VR-05-0131 Dated: November 6, 2005 Version: 1.1

9.2 Acronyms and Glossary

Acronyms

ADAM	Active Directory Application Mode
API	Application Programming Interface
CARP	Cache Array Routing Protocol

CC	Common Criteria
COM	Component Object Model
DLL	Dynamic Linked Library
EAL	Evaluation Assurance Level
EE	Enterprise Edition
GUI	Graphical User Interface
HLD	High Level Design
IT	Information Technology
LAT	Local Address Table
MIME	Multipurpose Internet Mail Extensions
MMC	Microsoft Management Console
MMS	Microsoft Media Streaming
MSDE	Microsoft Database Engine
MSDN	Microsoft Developer Network
NAT	Network Address Translation
NDIS	Network Driver Interface Specification
NIC	Network Interface Card
NLB	Network Load Balancing
ODBC	Open Database Connectivity
OWA	Outlook Web Access
PNM	RealNetworks Streaming Media Protocol
PP	Protection Profile
RAS	Remote Access Service
RTSP	Real Time Streaming Protocol
SE	Standard Edition
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SPI	Stateful Packet Inspection
SSL	Secure Socket Layer
SSP	Security Support Providers
SSPI	Security Support Provider Interface
ST	Security Target
TLS	Transport Layer Security

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
URI	Universal Resource Identifier
VPN	Virtual Private Network

Glossary

Active Directory	Active Directory is a so called Directory Service. It promises to support a single unified view of objects on a network and allows locating and managing resources faster and easier.
ADAM	ADAM is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service, rather than as a system service. Active Directory Application Mode (ADAM) is a part of Microsoft's fully integrated directory services available with Windows Server 2003, and is built specifically to address directory-enabled application scenarios. ADAM runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service means that multiple instances of ADAM can run concurrently on a single server, and each instance can be configured independently.
ADAM Configuration Receiver	The configuration is replicated from ADAM to the registry and file system by a service called ADAM Configuration Receiver Service.
application filters	Application filters can access the datastream or datagrams associated with a session within the Firewall service and work with some or all application-level protocols.
authentication	Authentication is "A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified." In simpler terms, it is "The act of verifying the claimed identity of an individual, station or originator" [Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)]
base-64	Encoding scheme for characters
Basic authentication	Basic authentication is the standard authentication method for Hypertext Transfer Protocol (HTTP). Though user information is encoded, no encryption is used with basic authentication.
broadcast network	A broadcast network (like Ethernet) has a local address for the interface and a broadcast address for the local subnet.
callback function	A callback function is installed by a client application to be notified when a special event occurs (the client is “called back”).
client (computer) set	a set of specific computers
credentials	An authentication method used to validate client-to-server and server-to-server communication. Credentials include a user name and a password

	that is used to validate requests from client computers or from other computers in an array or chain.
dynamic filters	Dynamic filters are automatically started by the Firewall service, Web proxy, or SOCKS proxy service. This feature allows the ISA services to automatically open and close communication ports on the external interface when transmission of packets is needed.
Feature Pack	A collection of feature extensions for a specific Microsoft product.
Firewall service	Firewall service is a Windows service that supports requests from firewall and Secure network address translation (SecureNAT) clients.
firewall service log file	contains entries with connection establishments and terminations
forward scenario	internal clients accessing the internet
hook function	A hook is an application-defined callback function that the system calls in response to events generated by an accessible object. The hook function processes the event notifications as required.
HTTP filter	A Hypertext Transfer Protocol (HTTP) filter provided with ISA, that forwards HTTP requests from Firewall and secure network address translation clients to the Web Proxy service.
Identification	Identification, according to a current compilation of information security terms, is "the process that enables recognition of a user described to an automated data processing system. This is generally by the use of unique machine-readable names" [Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)].
inbound	see “incoming”
inbound access	Ability to send information from an external network, such as the Internet, to an internal or external network.
incoming (traffic)	(traffic) from the external to the internal network interface
Integrated Windows authentication	formerly named NTLM or Windows NT Challenge/Response authentication
IP packet filters	IP packet filters allow or deny traffic on the packet layer.
ISA Server 2004	Microsoft Internet Security and Acceleration Server 2004
Kerberos	authentication protocol (http://www.ietf.org/rfc/rfc1510.txt)
load balancing	In a load balancing scheme, requests are forwarded to another server with more capacity, if one server starts to get unavailable because of the number of requests.
loopback network	A loopback network allows an application to connect on a local service (this is address 127.0.0.1 normally).
MMC	Microsoft Management Console – A configuration management tool supplied with Windows that can be extended with plugins.
MSP NAT Director	MS Proxy NAT Redirector
Network interface card (NIC)	A NIC or Network Interface Card is a circuit board or chip, which allows the computer to communicate to other computers on a Network.
NTLM	NTLM is an authentication scheme used by Microsoft browsers, proxies, and servers (Microsoft Internet Explorer, Internet Information Server and others). This scheme is also sometimes referred to as the NT

	challenge/response (NTCR) scheme or Integrated Windows authentication.
outbound	see “outgoing”
outbound access	Ability to send information from an internal or internal network to an external network, such as the Internet.
outgoing (traffic)	(traffic) from the internal to the external network interface
packet filter log file	contains records of packets that were dropped / allowed
packet traffic	packet traffic is sent on layer 2
padding	One or more bits appended to data in order to ensure that is contains the required number of bits and bytes.
policy rules traffic	Firewall traffic which is passes the Policy Rules (i.e. Access Rules, Publishing Rules and so on)
port number	A number that identifies a certain Internet application with a specific connection.
principal (security principal)	An entity recognized by the security system. Principals can include human users as well as autonomous processes.
Protocol rules	Protocol rules indicate whether a particular protocol is accessible for inbound and outbound communication.
publishing rules	publish virtually any computer on an internal network to the Internet (see Web publishing and Server publishing)
RADIUS	Remote Authentication Dial In Service (RADIUS), see [RADIUS] for details
remote procedure call (RPC)	A message-passing facility that allows a distributed application to call services available on various computers in a network. Used during remote administration of computers.
reverse scenario	publishing scenario / publishing internal servers to the internet
Scalability	The possibility to increase performance of an installation by adding additional systems.
Schannel	A security package (SSP) that provides authentication between clients and servers.
Secure Sockets Layer (SSL)	A protocol that supplies secure data communication through data encryption and decryption. SSL enables communications privacy over networks.
SecureNAT	Client computers that do not have Firewall Client software are SecureNAT clients. Although SecureNAT clients do not require special software, it is required to configure the default gateway so that all traffic destined to the Internet is sent by way of ISA Server, either directly or indirectly, through a router. Clients can be configured either by using the Dynamic Host Configuration Protocol (DHCP) service or manually. Strictly speaking SecureNAT clients are clients that are behind the firewall via Network Address Translation. Since ISA Server extends the network address translation (NAT) functionality, so all ISA Server rules can be applied to SecureNAT clients, and even though NAT does not have an inherent authentication mechanism, it is possible with ISA Server. Policies regarding protocol usage, destination, and content type are also applied to SecureNAT clients.

security context	The security attributes or rules that are currently in effect. For SSPI, a security context is an opaque data structure that contains security data relevant to a connection, such as a session key or an indication of the duration of the session.
security package	The software implementation of a security protocol. Security packages are contained in security support provider DLLs or security support provider/authentication package DLLs.
security principal	An entity recognized by the security system. Principals can include human users as well as autonomous processes.
Security Support Provider	A dynamic-link library that implements the SSPI by making one or more security packages available to applications. Each security package provides mappings between an application's SSPI function calls and an actual security model's functions. Security packages support security protocols such as Kerberos authentication and the Microsoft LAN Manager.
Server publishing	Server publishing allows virtually any computer on an internal network to publish to the Internet.
Service Pack	A collection of bug fixes for a specific Microsoft product.
Site and content rules	Site and content rules specify which sites and content can be accessed.
SSP	see Security Support Provider
SSPI	Security Support Provider Interface. A common interface between transport-level applications. SSPI allows a transport application to call one of several security providers to obtain an authenticated connection. These calls do not require extensive knowledge of the security protocol's details.
static filters	Filters that allow packets from other administrator-selected services from the Internet. A static filter is created during configuration of ISA by using the user interface. If IP packet filtering is enabled, the static filter is always on.
TLS	Transport Layer Security: TLS is based on the SSL 3.0 Protocol Specification
user agent	A user agent is also called “web proxy client” in ISA Server 2004. Normally a client that connects to web services is called “user agent” (for example a web browser).
UUID	Universal Unique Identifier - A UUID is an identifier that is unique across both space and time, with respect to the space of all UUIDs. A UUID can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects across a network.
W3C	World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) concerning Web technology (http://www.w3c.org)
Web listener	When you create a Web publishing rule, you specify a Web listener to be used when applying the rule. The Web listener properties determine the following: - Which Internet Protocol (IP) addresses and ports on the specified networks will listen for Web requests. - Which authentication method will be used, when authentication is

	required. - Number of connections that are allowed. Web listeners can be used by more than one Web publishing rule.
Web Proxy service	The Web Proxy service is a Windows service that supports requests from any Web browser. The Web Proxy service works at the application level on behalf of a client requesting an Internet object that can be retrieved using one of the protocols supported by the Web Proxy protocols: File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Gopher. The Web Proxy service also supports the Secure HTTP (HTTPS) protocol for secure sessions using Secure Sockets Layer (SSL) connections.
Web proxy service log file	stores one line per HTTP request
Web publishing	Web publishing publishes Web content to the Internet