Microsoft® Forefront™ Threat Management Gateway

# Forefront TMG 2010 Common Criteria Evaluation

## Security Target

*Microsoft Forefront Threat Management Gateway Team*


| | |
|---|---|
| Author: | Stephan Slabihoud, TÜVIT GmbH<br>Yossi Siles, Microsoft Corp.<br>Vladimir Holostov, Microsoft Corp.<br>Nady Gorodetsky, Microsoft Corp. |



| | |
|---|---|
| Version: | 1.1 |
| Last Saved: | 2010-12-13 |
| File Name: | MS_TMG_ST_1.1.docx |



### Abstract

This document is the ST (Security Target) of Forefront TMG Common Criteria Certification.



### Keywords

CC, ST, Common Criteria, Firewall, Security Target


### Revision History

| Date | Version | Author | Edit |
|---|---|---|---|
| 23-Sep-09 | 0.1 | Microsoft TMG Team | Created |
| 8-Oct-09 | 0.2 | Microsoft TMG Team | some additions |
| 26-Oct-09 | 0.3 | Microsoft TMG Team | some additions |
| 2-Nov-09 | 0.4 | Microsoft TMG Team | some additions |
| 3-Nov-09 | 0.5 | Microsoft TMG Team | some additions |
| 15-Dez-09 | 0.6 | Microsoft TMG Team | some additions |
| 25-Jan-10 | 0.7 | Microsoft TMG Team | some additions |
| 10-Feb-10 | 0.8 | Microsoft TMG Team | some additions |
| 1-Jun-10 | 0.9 | Microsoft TMG Team | some additions |
| 15-Jun-10 | 1.0 | Microsoft TMG Team | some additions |
| 13-Dec-10 | 1.1 | Microsoft TMG Team | some additions |

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 TOE overview summarizes the ST in narrative form and provides information for a potential user to determine whether Microsoft Forefront Threat Management Gateway (TMG) is of interest. The overview can also be used as a standalone abstract for ST catalogues and registers.

Forefront Threat Management Gateway is a further development of ISA Server 2006 that differs in four major ways:

- Secure Web Gateway: Forefront Threat Management Gateway can be used to protect internal users from Web-based attacks by integrating Web antivirus/anti-malware and URL filtering. With HTTPS inspection, it can even provide these protections in SSL-encrypted traffic.
- Improved Application Layer Defenses: Forefront Threat Management Gateway includes Network Inspection System, which enables protection against vulnerabilities found in Microsoft products and protocols.
- Improved Connectivity: Forefront Threat Management Gateway enhances its support for NAT scenarios with the ability to designate e-mail servers to be published on a 1-to-1 NAT basis. Additionally, Forefront Threat Management Gateway recognizes SIP traffic and supports SIP traversal across the firewall.
- Simplified Management: Forefront Threat Management Gateway has improved wizards to simplify its deployment as well as its continued configuration.

## 1.1 ST Reference

| | |
|---|---|
| ST Title: | *Forefront TMG* 2010 Common Criteria Evaluation - Security Target |
| ST Version: | 1.1 |
| ST Date: | 2010-12-13 |
| Cert. ID: | BSI-DSZ-CC-0670 |

## 1.2 TOE Reference

| | |
|---|---|
| TOE Identification: | *Microsoft Forefront Threat Management Gateway 2010 (CC)*<br>in its configurations<br>• *Standard Edition (English)*<br>• *Enterprise Edition (English)*<br>and its related guidance documentation |
| TOE Version: | 7.0.7734.100 |
| TOE Platform: | Windows Server 2008 R2 (English), 64-bit |
| CC Identification: | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3 as of July 2009 for parts 1, 2 and 3. ([CC]) |
| Evaluation Assurance Level: | EAL4 augmented by ALC_FLR.3 |
| PP Conformance: | none |

## 1.3 Overview

This chapter presents a general overview of Microsoft Forefront Threat Management Gateway (TMG)[1].

TMG is a secure Web gateway that helps protect employees from Web-based threats. It also delivers simple, unified perimeter security with integrated firewall, VPN, intrusion prevention, antivirus, and URL filtering. TMG is an integrated solution optimized for application-layer defense, stateful packet inspection (SPI), application-layer intrusion prevention, and offers integrated anti-malware and antivirus protection. TMG provides multi-networking support, virtual private networking configuration, extended and extensible user and authentication models, and improved management features.

TMG comprises the network-layer attack prevention and application-layer intrusion detection, certain identification and authentication mechanism as part of protocols included, and audit functionality.

TMG can be installed as a dedicated (software) firewall that runs on Windows Server operating system. It acts as the secure gateway to the Internet for internal clients and protects communication between internal computers and the Internet. It is available in two configurations[2]: Standard Edition (single machine support only) and Enterprise Edition (for large-scale deployments).

As a multilayered firewall, TMG provides security at different levels. IP packet filtering provides security by inspecting individual packets passing through the firewall. Application-level filtering allows TMG to intelligently inspect and secure popular protocols (such as HTTP, and others).

[1] short: ”TMG”

[2] for details refer to chapter 1.4.1

TMG 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. This reduces the number of communication ports that are statically open to inbound connections.

With TMG'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. TMG 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. These logs can be configured and enabled for packet and application filtering. They are human readable and can be reviewed with additional tools.

## 1.4 TOE Overview and description

The TOE is the main part of TMG (the logical scope and boundary are described in chapter 1.4.3) that helps to provide secure Internet connectivity. It is an integrated solution for application-layer defense, stateful packet inspection, and secure web publishing. TMG can be installed as a dedicated (software) firewall that runs on Windows 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 TOE can be configured that only particular users are allowed to access Web applications through the TOE. In a publishing scenario it is possible that a user authenticates once and gains access to multiple resources (web applications). The TOE also features detailed security and access logs and provides the ability to perform filter, search and sort operations on the recorded audit data.

The operation system Windows Server maintains security attributes for all administrators. Windows 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 functionalities of the TOE.

### 1.4.1 Available TOE configurations

There are two configurations of TMG 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.

TMG 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. The Standard Edition can be managed centrally from an enterprise deployment. In the Standard Edition there is a single-server array only that inherits the enterprise policy.

In both Standard Edition and Enterprise Edition the policy configuration data is stored in ADAM (a Lightweight Directory Access Protocol (LDAP) directory service)[3]. 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 and not started by default.

Both configurations - 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 are outside the scope of the TOE) and also scalability is not part of the evaluation. It is also possible to change the configuration from “Standard” to “Enterprise”[4].

Note:

To avoid confusion, “configuration” has been used instead of “version”. So there is one version of TMG which can be installed in two configurations: Standard Edition and Enterprise Edition. The configuration is chosen by executing the corresponding setup (Standard Edition setup or Enterprise Edition setup).

Standard Edition and Enterprise Edition of TMG have been considered in this Security Target.

[3] http://www.microsoft.com/windowsserver2003/adam/

[4] http://technet.microsoft.com/en-us/library/dd896980.aspx

### 1.4.2 Physical scope and boundary

The TOE consists of following two configurations:

a) “Standard Edition”, which consists of:

- A software package “Microsoft Forefront Threat Management Gateway 2010 – Standard Edition” (English) - delivered on DVD-ROM (boxed version) and downloadable from the web (volume license),
- A manual (a Windows Help File) [MSTMG] - delivered as part of the software package and installed on the host system with the TOE,
- A Guidance Addendum [MSTMG_ADD] - delivered via the TMG product page [WEBTMG].

b) “Enterprise Edition”, which consists of:

- A software package “Microsoft Forefront Threat Management Gateway 2010 – Enterprise Edition” (English) - downloadable from the web (volume license),
- A manual (a Windows Help File) [MSTMG] - delivered as part of the software package and installed on the host system with the TOE,
- A Guidance Addendum [MSTMG_ADD] - delivered via the TMG product page [WEBTMG].

Each configuration can run on a single machine, which comprises the evaluated TOE and non evaluated components.

The TOE (in both configurations) is running on an

- Windows Server 2008 R2 (English), 64-bit

which has been used as underlying operating system for evaluation.

The TOE relies on functionality of the Windows Server Operating System and has the following hardware/software requirements:

**Table 1.1 – Minimum Hardware Requirements**

| Aspect | Requirement |
|---|---|
| CPU | 64bit, dual core |
| RAM | 2 GB |
| Hard Disk | Approx 2500 MB of free space, NTFS formatted |
| Other | One network adapter that is compatible with the computer’s operating system, for communication with the Internal network. An additional compatible network adapter for each network connected to the Forefront TMG computer. |

The evaluated functionality respectively the TOE (the logical scope) is stated in the following chapter 1.4.3. In particular Figure 1.1 shows the demarcation of the TOE respectively TMG.

### 1.4.3 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
- Information Flow Control
- Audit

#### 1.4.3.1 Web Identification and Authentication

The TOE can be configured that only particular users are allowed to access Web applications that reside in a corporate (internal) network through the TOE after a successful authentication ("Web publishing" rules[5] use the local Windows Server database or a Radius server to authenticate users for Web access). Single-Sign-On allows a user to authenticate once and gain access to multiple resources (web applications) and, as much as possible, without requiring special features in the web applications the user accesses.

In the **Front-End Authentication** process the user authentication information is send to TMG (basically the Front-Base Authentication provides the interface a user will see in the web browser). The **Gateway Authentication** process TMG performs with the gateway authentication provider is done in order to verify that the user authentication information is correct. In the **Backend authentication** process TMG authenticates the session on behalf of the user (the TOE connects to the internal resource and uses the provided credentials from the Front-End Authentication to authenticate the user).

For all three authentication steps different authentication methods can be chosen. Chapter 7.1 gives an overview about supported and evaluated authentication methods.

#### 1.4.3.2 Information Flow Control

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:

##### 1.4.3.2.1 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.

[5] see chapter 1.4.3.2, chapter 7.2.1.4 and glossary

**Network rules (NAT and route)**

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.

**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 SF2 (chapter 7.2) 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 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 TMG cache (which is not evaluated).

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

#### 1.4.3.2.2 Web- and Application filters

TMG application filters provide an extra layer of security. Web- and Application filters can access the data stream or datagrams associated with a session. Web- and Application filters

are registered with the Firewall service (a service installed by TMG) 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[6].

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 TMG.

Web filters supported by the TOE are: Form-based Authentication Filter, Authentication Delegation Filter, and URL Filtering.

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

#### 1.4.3.2.3 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.

#### 1.4.3.2.4 Lockdown mode

The TOE's lockdown feature combines the need for isolation with the need to stay connected for maintenance. Whenever a situation occurs that causes the Firewall service to shut down, the TOE enters the lockdown mode.

#### 1.4.3.2.5 Policy Re-evaluation

Existing client connections will be reevaluated when the existing policy gets modified. Client connections not matching the newly enforced policy will be dropped.

### 1.4.3.3 Audit

The TOE features detailed security and access logs (firewall service log file and web proxy log file). For evaluation the SQL Server Express database based 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, search and sort operations on the recorded audit data. Policy-change auditing allows following policy rules changes.

Important system events and failures are logged in the Windows application event log.

## 1.4.4 TOE Demarcation Summary

For better understanding the boundaries of the TOE are summarized in Figure 1.1. It shows the TOE with its three security functionalities:

- Web Identification & Authentication,

[6] such as authentication and virus checking

- Information Flow Control,
- Audit.

The additional features of TMG are not part of the evaluation: Web Cache, GUI (except Log Viewer component), RAS & VPN, Storage Service, ADAM Configuration Receiver, Network Inspection[7], Load Balancing (incl. Web Publishing Load Balancing), other Management and Identification & Authentication functionality (like Wizards and Authentication Methods), Extensibility Features, some protocol filters (not mentioned in the picture below) and the used functionalities of the underlying operating system Windows 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 SQL Server Express 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” 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 TMG, since TMG in the configuration “Enterprise Edition” provides NLB functionality (not evaluated).

For information purpose and better understanding the interfaces between

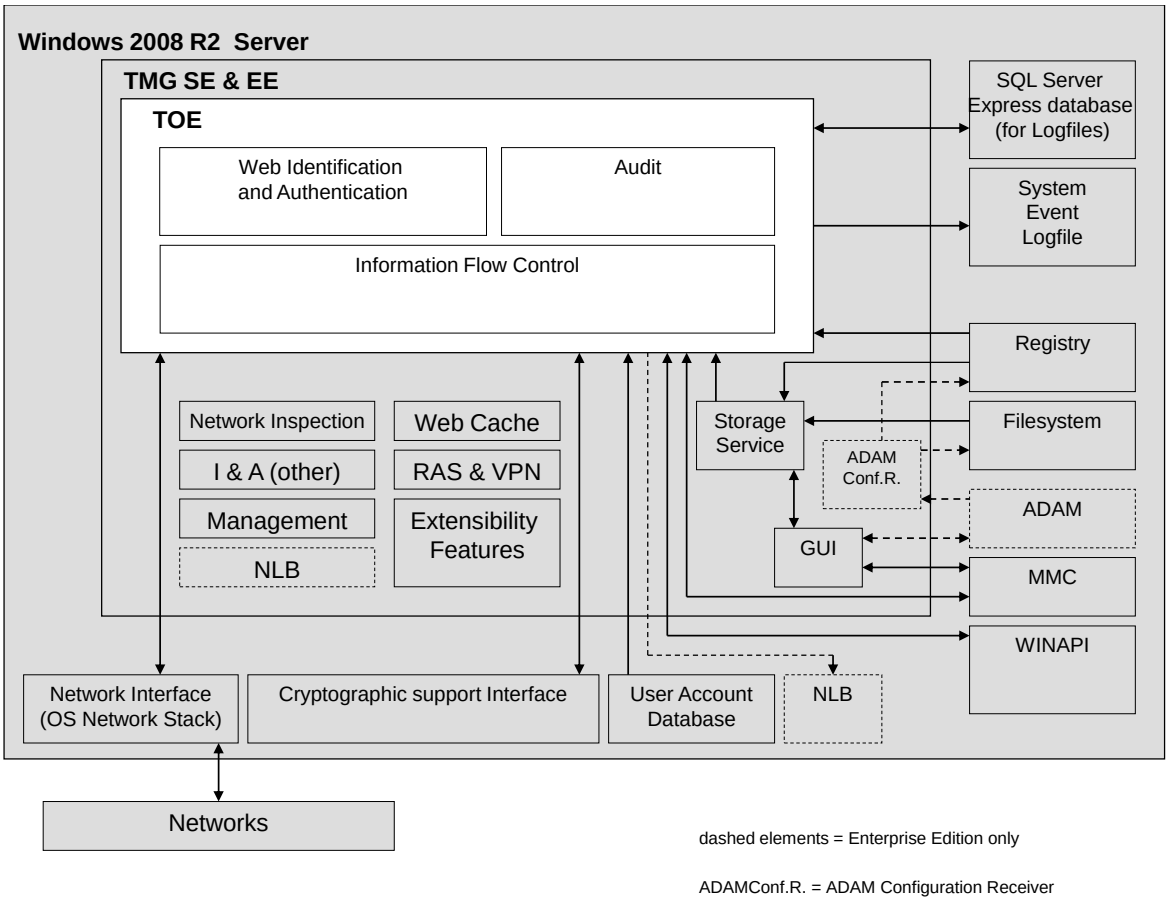
- GUI and Storage Service, GUI and MMC, GUI and ADAM,
- Storage Service and Registry, Storage Service and Filesystem, and
- ADAM Configuration Receiver and ADAM, ADAM Configuration Receiver and Filesystem, ADAM Configuration Receiver and Registry,

are also shown in the picture below.

Dashed elements shown in the picture are used within TMG Enterprise Edition. All other elements are identical in TMG Standard Edition and Enterprise Edition.

[7] can be used as IPS (Intrusion Prevention) and IDS (Intrusion Detection)

**Figure 1.1 – TOE demarcation**




## 1.5 Conventions

For this Security Target the following conventions are used:

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in part 1 of [CC]. The following conventions are used in this ST:

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by prefix “refinement”.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made are denoted by prefix “selection”.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made are denoted by prefix “assignment”.

The **iteration** operation is used when a component is repeated with varying operations. Iterations are indicated by the use of parentheses “()” in the component identification and by parentheses “()” and an abbreviation in the component name.

The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed ‘explicit requirements’ and are permitted if the CC does not offer suitable requirements to meet the authors’ needs.

**Explicit requirements** must be identified and are required to use the CC class/family/component model in articulating the requirements. In this ST, explicit requirements will be indicated with the prefix “EXT_” followed by the component name.

# 2 Conformance Claims

This chapter contains the following sections:

- CC conformance claims
- PP claim
- Package claim

## 2.1 CC Conformance Claims

This Security Target claims to be conformant to the Common Criteria 3.1:

- Part 2 extended to [CC, Part 2]

  In order to provide a complete description of the functional requirements addressed by the TOE, functional components of part 2 of the Common Criteria framework were used. But also additions to the Common Criteria part 2 were defined, to fulfill the requirement of a complete and consistent TOE description.

- Part 3 conformant to [CC, Part 3]

  For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 were used.

## 2.2 Package Claim

This ST claims to be conformant to the assurance requirements package EAL4 augmented by ALC_FLR.3.

## 2.3 PP Claim

This ST does not claim conformance to any PP.

# 3 Security Problem Definition

This chapter aims to clarify the security problems that TMG is intended to solve, by describing any assumptions and organizational security policies 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.

## 3.1 Assets

The assets under attack are: internal IT entities which are protected by the TOE. In general, the threat agent (attacker) includes, but is not limited to:

- Non authorized persons or
- External IT entities not authorized to use the TOE itself.

## 3.2 Threats

Threats to the TOE are defined in Table 3.1 below.

**Table 3.1 – Threats**

| # | Threat | Description |
|---|---|---|
| 1 | T.NOAUTH | An attacker may attempt to bypass the security of the TOE so as to access and use security functionality and/or non-security functionality provided by the TOE.<br>The TOE provides Form-based 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 functionality (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 attackers' actions. This might be a result of a strange denial of service attack. |

## 3.3 Organizational 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. |

## 3.4 Assumptions

Table 3.3 lists the TOE Secure Usage Assumptions for the IT and non-IT environment and intended usage.

**Table 3.3 – 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 operating system implements following functionality:<br>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 (for EE configuration only), Network Load Balancing (for EE configuration only, 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 cannot flow among the internal and external networks unless it passes through the TOE. |

| # | Assumption Name | Description |
|---|---|---|
| 8 | A.WEBI&A | User credentials are verified optionally by a Radius Server. The Radius Server returns a value if a valid account exists or not.<br><br>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 Form-based authentication have to be configured by the administrator so that a secure connection is enforced. |
| 10 | A.URLFILTER | TMG queries the remotely hosted Microsoft Reputation Service to determine the categorization of the Web site.<br><br>The download of the Reputation Service data is appropriately secured with respect to the integrity and authenticity. |

# 4 Security Objectives

This chapter contains the following sections:

- Security objectives for the TOE
- Security objectives for the operational environment
- Security objectives rationale

## 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 Form-based 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 insufficient storage capacity. |
| 5 | O.ACCOUN | The TOE must provide user accountability for information flows through the TOE. |

## 4.2 Security objectives for the operational 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 operating system should implement following functionality:<br>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 (for EE configuration only), Network Load Balancing (for EE configuration only, 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 | Optionally a Radius Server should verify provided user credentials and return if a valid account exists or not.<br>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 Form-based authentication should be configured by the administrator so that a secure connection is enforced. |
| 10 | OE.URLFILTER | TMG queries the remotely hosted Microsoft Reputation Service to determine the categorization of the Web site.<br>The download of the Reputation Service data is appropriately secured with respect to the integrity and authenticity. |

## 4.3 Security objectives rationale

This table maps assumptions, threads, and OSPs to objectives, demonstrating that all assumptions, threats, and OSPs are mapped to at least one objective and vice versa. A discussion of the rationale for the mappings is provided below.

**Table 4.3 – Security Objectives rationale**

| Threats and Assumptions vs. Security Objectives | O.IDAUTH | O.MEDIAT | O.SECSTA | O.AUDREC | O.ACCOUN | OE.PHYSEC | OE.GENPUR | OE.NOEVIL | OE.SINGEN | OE.DIRECT | OE.SECINST | OE.ENV | OE.WEBI&A | OE.SSL | OE.URLFILTER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **T.NOAUTH** | X | | X | | | | | | | | | | | | |
| **T.MEDIAT** | | X | | | | | | | | | | | | | |
| **T.OLDINF** | | X | | | | | | | | | | | | | |
| **T.AUDFUL** | | | | X | | | | | | | | | | | |
| **P.AUDACC** | | | | X | X | | | | | | | | | | |
| **A.PHYSEC** | | | | | | X | | | | | | | | | |
| **A.GENPUR** | | | | | | | X | | | | | | | | |
| **A.NOEVIL** | | | | | | | | X | | | | | | | |
| **A.SINGEN** | | | | | | | | | X | | | | | | |
| **A.DIRECT** | | | | | | | | | | X | | | | | |
| **A.SECINST** | | | | | | | | | | | X | | | | |
| **A.ENV** | | | | | | | | | | | | X | | | |
| **A.WEBI&A** | | | | | | | | | | | | | X | | |
| **A.SSL** | | | | | | | | | | | | | | X | |
| **A.URLFILTER** | | | | | | | | | | | | | | | X |

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 functionalities and/or non-security functionalities 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 functionalities related to audit.

# 5 Extended Components Definition

This chapter defines TOE security functional requirements which are not part of CC 3.1 part 2. No security assurance requirements extended components exist.

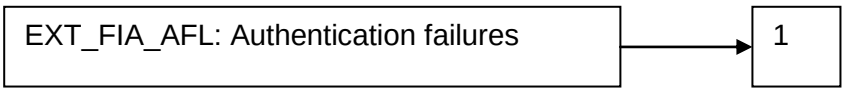
## 5.1 Definition of functional family EXT_FIA_AFL

### 5.1.1 EXT_FIA_AFL Authentication failures

Family Behavior:

This family contains requirements for defining values to specify the number of unsuccessful authentication attempts and the TSF actions in cases of authentication attempt failures. Parameters include, but are not limited to, the number of failed authentication attempts and time thresholds.

Component leveling:




EXT_FIA_AFL.1 Authentication failure handling, requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs.

Management: EXT_FIA_AFL.1

The following actions could be considered for the management functions in FMT:

a) management of the threshold for unsuccessful authentication attempts;

b) management of actions to be taken in the event of an authentication failure.

Audit: EXT_FIA_AFL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).

**EXT_FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

**EXT_FIA_AFL.1.1** **The TSF shall detect when [*selection: [assignment: positive integer number*], *an administrator configurable positive integer within* [*assignment*: *range of acceptable values*]] unsuccessful authentication attempts occur related to [*assignment: list of authentication events*].**

**EXT_FIA_AFL.1.2** **When the defined number of unsuccessful authentication attempts has been [*selection: met or surpassed*], the TSF shall [*assignment: list of actions*].**

**EXT_FIA_AFL.1.3** **The TOE shall handle the authentication failure after the verification has failed.**

Dependencies: EXT_FIA_UAU.1 Timing of authentication

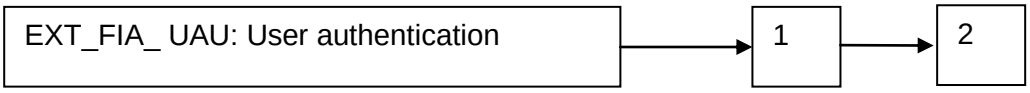
## 5.2 Definition of functional family EXT_FIA_UAU

### 5.2.1 EXT_FIA_UAU User authentication

Family Behavior:

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

Component leveling:




EXT_FIA_UAU.1 Timing of authentication, allows a user to actions prior to the authentication of the user's identity.

EXT_FIA_UAU.2 User authentication before any action, requires authenticated before any action will be allowed by the TSF.

Management: EXT_FIA_UAU.1

The following actions could be considered for the management functions in FMT:

a) management of the authentication data by an administrator;

b) management of the authentication data by the associated user;

c) managing the list of actions that can be taken before the user is authenticated.

Management: EXT_FIA_UAU.2

The following actions could be considered for the management functions in FMT:

a) management of the authentication data by an administrator;

b) management of the authentication data by the user associated with this data.

Audit: EXT_FIA_UAU.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Unsuccessful use of the authentication mechanism;

b) Basic: All use of the authentication mechanism;

c) Detailed: All TSF mediated actions performed before authentication of the user.

Audit: EXT_FIA_UAU.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Unsuccessful use of the authentication mechanism;

b) Basic: All use of the authentication mechanism.

**EXT_FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

**EXT_FIA_UAU.1.1 The TSF shall allow [*assignment: list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.**

**EXT_FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

Dependencies: EXT_FIA_UID.1 Timing of identification

**EXT_FIA_UAU.2 User authentication before any action**

Hierarchical to: EXT_FIA_UAU.1 Timing of authentication

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.

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

Dependencies: EXT_FIA_UID.1 Timing of identification

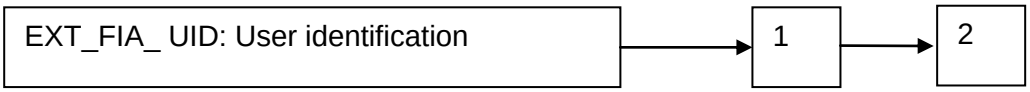
## 5.3 Definition of functional family EXT_FIA_UID

### 5.3.1 EXT_FIA_UID User identification

Family Behavior:

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

Component leveling:




EXT_FIA_UID.1 Timing of identification, allows users to perform certain actions before being identified by the TSF.

EXT_FIA_UID.2 User identification before any action, requires that users identify themselves before any action will be allowed by the TSF.

Management: EXT_FIA_UID.1

The following actions could be considered for the management functions in FMT:

a) the management of the user identities;

b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.

Management: EXT_FIA_UID.2

The following actions could be considered for the management functions in FMT:

a) the management of the user identities.

Audit: EXT_FIA_UID.1, EXT_FIA_UID.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;

b) Basic: All use of the user identification mechanism, including the user identity provided.

**EXT_FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

**EXT_FIA_UID.1.1** **The TSF shall allow [*assignment: list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.**

**EXT_FIA_UID.1.2** **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

Dependencies: No dependencies.

**EXT_FIA_UID.2 User identification before any action**

Hierarchical to: EXT_FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies.

# 6 Security Requirements

## 6.1 Security Functional Requirements

This chapter defines the TOE security functional requirements. A list of the requirements is provided in Table 6.1. The full text of the security functional requirements is listed below.

**Table 6.1 – 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.1 |
| 6 | EXT_FIA_UAU.2 | User authentication before any action | EXT_FIA_UID.1 |
| 7 | EXT_FIA_UID.2 | User identification before any action | none |
| **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_IFC.1 (4) | Subset information flow control (4) - URL FILTER SFP | FDP_IFF.1 (4) |
| 12 | FDP_IFF.1 (1) | Simple security attributes (1) - UNAUTHENTICATED SFP | FDP_IFC.1 (1)<br>FMT_MSA.3 |
| 13 | FDP_IFF.1 (2) | Simple security attributes (2) - UNAUTHENTICATED_APPL SFP | FDP_IFC.1 (2)<br>FMT_MSA.3 |
| 14 | FDP_IFF.1 (3) | Simple security attributes (3) - AUTHENTICATED SFP | FDP_IFC.1 (3)<br>FMT_MSA.3 |
| 15 | FDP_IFF.1 (4) | Simple security attributes (4) - URL FILTER SFP | FDP_IFC.1 (4)<br>FMT_MSA.3 |
| 16 | FDP_RIP.1 | Subset residual information protection | none |
| 17 | FMT_MSA.3 | Static attribute initialization | FMT_MSA.1<br>FMT_SMR.1<br>FMT_SMF.1 |

Note:
FPT_STM.1, FAU_STG.1, FMT_MSA.1, FMT_SMR.1 and FMT_SMF.1 are related to the IT environment.

### 6.1.1 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 6.2].

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 6.2].

**Table 6.2 – Auditable Events**

| Functional Component | Level | Auditable Event | Additional Audit Record Contents |
|---|---|---|---|
| EXT_FIA_UAU.2 | basic | All use of the user authentication mechanism. | The user identities provided to the TOE |
| EXT_FIA_UID.2 | basic | All use of the user identification 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. |
| FDP_IFF.1 (4) | minimal | Decisions to permit requested information flows. | The presumed URL of the 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 FMT_SMF.1 “Minimal: Use of the management functions.” is not part of the TOE (the functional component FMT_SMF.1 is part of the environment). The management functions for configuration and auditing are provided by the underlying operating system.

The TOE supports two mode of operation: Normal mode and Lockdown mode. In Lockdown mode (see chapter 7.2.5) 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.

Application note:

The TOE preprocesses the audit data in order to allow the MMC to display the items.

**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*].

Application note:

The TOE preprocesses the audit data in order to allow the MMC to display the filtered, selected or ordered items.

**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*].

## 6.1.2 Class FIA – Identification and authentication

**EXT_FIA_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

EXT_FIA_AFL.1.1 The TSF shall detect when [*selection:* [*assignment: one*]] unsuccessful authentication attempts occur related to [*assignment: failed Form-based authentication*].

EXT_FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*selection: met*], the TSF shall [*assignment: create a log file entry*].

EXT_FIA_AFL.1.3 The TOE shall handle the authentication failure after the verification has failed.

Dependencies: EXT_FIA_UAU.1 Timing of authentication

Note:

Form-based authentication is used in the in the Front-End Authentication process (see chapter 7.1 for more information).

Unlike FIA_AFL.1 (component from CC part 2) the required verification of the user credentials is done outside this component and thus part of the environment.

**EXT_FIA_UAU.2 User authentication before any action**

Hierarchical to: EXT_FIA_UAU.1 Timing of authentication

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.

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

Dependencies: EXT_FIA_UID.1 Timing of identification

Note:

The authentication data is stored in a cookie on the clients' system. This allows a user to authenticate once (referenced as "Single-Sign-On" process) and gain access to multiple resources (web applications).

The verification of the user credentials is done in the Gateway Authentication process (see chapter 7.1 for more information).

Unlike FIA_UAU.2 (component from CC part 2) the required verification of the user credentials done by local operating system or Radius server is done outside this component and thus part of the environment.

**EXT_FIA_UID.2 User identification before any action**

Hierarchical to: EXT_FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies.

Note:

Verification of the user credentials is done in the Gateway Authentication process (see chapter 7.1 for more information).

Unlike FIA_UID.2 (component from CC part II) the required verification of the user credentials done by local operating system or Radius server is done outside this component and thus part of the environment.

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.

## 6.1.3 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_IFC.1 Subset information flow control (4) – URL FILTER SFP**

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

[*assignment:*

*a) subjects: external IT entities that send and receive HTTP(S) information through the TOE to one another.*

*b) information: HTTP(S) traffic sent through the TOE via the URL FILTER from one subject to another;*

c) *operation: 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) 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_IFF.1 Simple security attributes (4) – URL FILTER SFP**

FDP_IFF.1.1 (4) The TSF shall enforce the [*assignment: URL FILTER SFP*] based on the following types of subject and information security attributes:

[*assignment:*

a) *subject attributes:*

*presumed URL;*

b) *information attributes:*

a. *presumed URL;*

b. *services: HTTP, HTTPS*].

FDP_IFF.1.2 (4) 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 URL in the information translates to an internal network address;*

*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 URL in the information translates to an external network address*]

FDP_IFF.1.3 (4) The TSF shall enforce the [*assignment: none*].

FDP_IFF.1.4 (4) The TSF shall provide the following [*assignment: none*].

FDP_IFF.1.5 (4) The TSF shall explicitly authorize an information flow based on the following rules: [*assignment: none*].

FDP_IFF.1.6 (4) The TSF shall explicitly deny an information flow based on the following rules:

[*assignment:*

*The presumed URL is part of the blocked category which is requested from the Microsoft Reputation Service (MRS) and not overridden locally.]*]

**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*].

## 6.1.4 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.

The management functions for configuration and auditing are provided by the underlying operating system, so FMT_SMF.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, AUTHENTICATED SFP, and URL FILTER*] 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. |

## 6.2 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.3 (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 6.3. Augmented assurance requirements have been printed in bold.

**Table 6.3 – EAL4 (augmented) Assurance Requirements**

| **Assurance Component** | **Name** |
|---|---|
| ADV_ARC.1 | Security architecture description |
| ADV_FSP.4 | Complete functional specification |
| ADV_IMP.1 | Implementation representation of the TSF |
| ADV_TDS.3 | Basic modular design |
| AGD_OPE.1 | Operational user guidance |
| AGD_PRE.1 | Preparative procedures |
| ALC_CMC.4 | Production support, acceptance procedures and automation |
| ALC_CMS.4 | Problem tracking CM coverage |
| ALC_DEL.1 | Delivery procedures |
| ALC_DVS.1 | Identification of security measures |
| **ALC_FLR.3** | **Systematic flaw remediation** |
| ALC_LCD.1 | Developer defined life-cycle model |
| ALC_TAT.1 | Well-defined development tools |
| ASE_CCL.1 | Conformance claims |
| ASE_ECD.1 | Extended components definition |
| ASE_INT.1 | ST introduction |
| ASE_OBJ.2 | Security objectives |

| Assurance Component | Name |
|---|---|
| ASE_REQ.2 | Derived security requirements |
| ASE_SPD.1 | Security problem definition |
| ASE_TSS.1 | TOE summary specification |
| ATE_COV.2 | Analysis of coverage |
| ATE_DPT.1 | Testing: security enforcing modules |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing - sample |
| AVA_VAN.3 | Focused vulnerability analysis |

## 6.3 Security Requirement Rationale

The following chapters contain the security requirement rational.

### 6.3.1 Rationale for the security functional requirements

The mapping of security objectives to functional requirements (components) is provided in Table 6.4.

**Table 6.4 – Security Objective to SFR**

| Security Objectives vs. Functional Component | O.IDAUTH | O.MEDIAT | O.SECSTA | O.AUDREC | O.ACCOUN |
|---|---|---|---|---|---|
| **EXT_FIA_AFL.1** | X | | | | |
| **EXT_FIA_UID.2** | X | | | | X |
| **EXT_FIA_UAU.2** | X | | | | X |
| **FDP_IFC.1 (1)** | | X | | | |
| **FDP_IFC.1 (2)** | | X | | | |
| **FDP_IFC.1 (3)** | | X | | | |
| **FDP_IFC.1 (4)** | | X | | | |
| **FDP_IFF.1 (1)** | | X | | | |
| **FDP_IFF.1 (2)** | | X | | | |
| **FDP_IFF.1 (3)** | | X | | | |
| **FDP_IFF.1 (4)** | | X | | | |
| **FDP_RIP.1** | | X | | | |
| **FMT_MSA.3** | | X | X | | |

| Security Objectives vs. Functional Component | O.IDAUTH | O.MEDIAT | O.SECSTA | O.AUDREC | O.ACCOUN |
|---|---|---|---|---|---|
| **FAU_GEN.1** | | | | X | X |
| **FAU_SAR.1** | | | | X | |
| **FAU_SAR.3** | | | | X | |
| **FAU_STG.3** | | | | X | |

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 Form-based 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. The Form-based 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_IFC.1 (4), FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_IFF.1 (3), FDP_IFF.1 (4), 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_IFC.1 Subset information flow control (4)

  This component identifies the entities involved in the information flow control URL FILTER SFP. HTTP(S) data transferred must pass the URL filter.

- 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.

- FDP_IFF.1 Simple security attributes (4)

  This component identifies the attributes of the users sending and receiving the information in the URL FILTER SFP, as well as the attributes for the information itself. Then the policy is defined under which conditions information 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.

- 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.

**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 using 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 functionalities 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 Form-based 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. The Form-based 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).

### 6.3.2 Dependencies of security functional requirements

**Table 6.5 – TOE Functional Requirements Dependencies**

| # | **Requirement (SFR TOE)** | **Dependencies** | **Dependency fulfilled** |
|---|---|---|---|
| 1 | FAU_GEN.1 | FPT_STM.1 | A.ENV |
| 2 | FAU_SAR.1 | FAU_GEN.1 | yes |
| 3 | FAU_SAR.3 | FAU_SAR.1 | yes |
| 4 | FAU_STG.3 | FAU_STG.1 | A.ENV |
| 5 | EXT_FIA_AFL.1 | EXT_FIA_UAU.1 | yes |
| 6 | EXT_FIA_UAU.2 | EXT_FIA_UID.1 | yes |
| 7 | EXT_FIA_UID.2 | none | yes |
| 8 | FDP_IFC.1 (1) – UNAUTHENTICATED SFP | FDP_IFF.1 (1) | yes |
| 9 | FDP_IFC.1 (2) – UNAUTHENTICATED_APPL SFP | FDP_IFF.1 (2) | yes |
| 10 | FDP_IFC.1 (3) – AUTHENTICATED SFP | FDP_IFF.1 (3) | yes |
| 11 | FDP_IFC.1 (4) – URL FILTER SFP | FDP_IFF.1 (4) | yes |
| 12 | FDP_IFF.1 (1) – UNAUTHENTICATED SFP | FDP_IFC.1 (1), FMT_MSA.3 | yes |
| 13 | FDP_IFF.1 (2) – UNAUTHENTICATED_APPL SFP | FDP_IFC.1 (2), FMT_MSA.3 | yes |
| 14 | FDP_IFF.1 (3) – AUTHENTICATED SFP | FDP_IFC.1 (3), FMT_MSA.3 | yes |
| 15 | FDP_IFF.1 (4) – URL FILTER SFP | FDP_IFC.1 (4), FMT_MSA.3 | yes |
| 16 | FDP_RIP.1 | none | yes |
| 17 | FMT_MSA.3 | FMT_MSA.1, FMT_SMF.1, FMT_SMR.1 | A.ENV |

All TOE Functional Requirements Dependencies are either fulfilled by the TOE Functional Requirement hierarchy, by a TOE SFR, or by the IT environment.

The timestamp is provided by the underlying operating system. So FPT_STM.1 is related to A.ENV.

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), FMT_MSA.1 (4), and FMT_SMR.1 are related to A.ENV.

The TOE does not provide management functionality. This is provided by the underlying operating system, so FMT_SMF.1 is related to A.ENV.

Access to the log files is restricted to authorized persons by the underlying operating system, so FAU_STG.1 is related to A.ENV.

### 6.3.3 Rationale for the assurance requirements

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 functionalities, using a functional and complete interface specification, guidance documentation, the TOE design specification, and a subset of the implementation, to understand the security behavior. AVA_VAN.3 provides resistance against attackers with enhanced basic attack potential and ensures that the evidence shows that the search for vulnerabilities is focused; the augmentation with ALC_FLR.3 ensures that the developer has documented a systematic 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, provide a flaw remediation procedure, a procedures for processing reported security flaws, and a flaw remediation guidance. Assurance is additionally gained through an informal model of the TOE security policy. The analysis is supported by independent testing of the TOE security functionalities, evidence of developer testing based on the functional specification and TOE design specification, selective independent confirmation of the developer test results, evidence of a developer search for vulnerabilities, and an focused vulnerability analysis demonstrating resistance to penetration attackers with an enhanced-basic 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.3) offer a complying level of assurance.

# 7 TOE Summary Specification

The TOE summary specification in the following specifies the security functionalities as well as the assurance measures of the TOE.

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

SF1: Web Identification and Authentication
- describes the authentication mechanism for web applications

SF2: Information Flow Control
- contains all filtering capabilities of the TOE.

SF3: Audit
- describes the audit capabilities

All Security functionalities are valid for both configurations, Standard Edition and Enterprise Edition, unless explicitly mentioned.

Note:

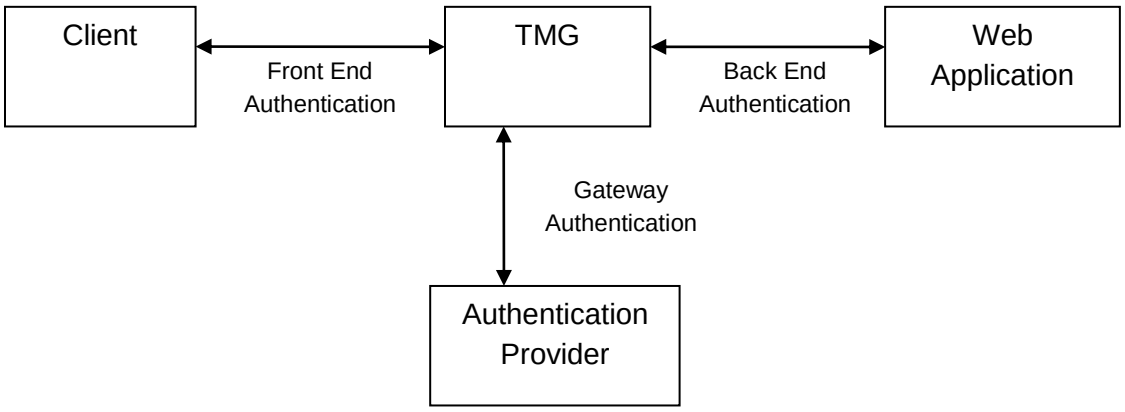
For the Standard Edition security policy configuration data is stored in the local Windows registry, for the Enterprise Edition security policy configuration data is stored in ADAM (a Lightweight Directory Access Protocol (LDAP) directory service)[8]. The configuration data is then replicated by a system service into the local Windows registry and file system.

## 7.1 SF1 – Web Identification and Authentication

The TOE can be configured that only particular users (which means all or selected users) are allowed to access Web applications in a corporate network through the TOE using Form Based Authentication (“Web publishing” rules; see 7.2.1 “Web publishing”, optionally secured by SSL encryption). Using Form Based Authentication a user can authenticate once and gain access to multiple resources (web applications) and, as much as possible, without requiring special features in the web applications the user accesses (that a user authenticates once to gain multiple access is also referred as “Single-Sign-On”).

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

**Figure 7.1 – Web Identification & Authentication Process (Single-Sign-On)**




In the **Front-End Authentication** process the user authentication information is send to TMG. In the evaluated version of TMG Form-based Authentication has to be used (FBA).

Form-based authentication is used when publishing web applications like Microsoft Outlook Web Access (OWA) servers. After the user provides user credentials in the form, the TOE issues a cookie, identifying the user. On subsequent requests, the system first checks the cookie to see if the user was already authenticated, so that the user does not have to supply credentials again. The credential information is not cached on the client computer, and is valid only during the current session. This is particularly important in a scenario where users are connecting to the Outlook Web Access server from public computers, where credentials are not wanted to be cached. Users are required to reauthenticate if they close the browser, log off from a session, or navigate to another Web site. Also, it is possible to configure a maximum idle session time-out, so that if a user is idle for a prolonged period of time, reauthentication is required.

The **Gateway Authentication** process TMG performs with the gateway authentication provider is done in order to verify that the user authentication information is correct.

In the **Backend authentication** process TMG authenticates the session on behalf of the user. This process is sometimes referred to as “basic delegation”. TMG performs HTTP Basic Authentication with the web application (Back End Authentication) and FBA with the Client (Front Base Authentication).

The following describes the authentication procedure where a user authenticates once and gains multiple access (also referred as **Single-Sign-On Session**): The TOE asks the client for user authentication only once at the beginning of a session (Front End Authentication). It gets the user name and password in clear text from a HTTP post-request and uses the data to get an impersonation token using

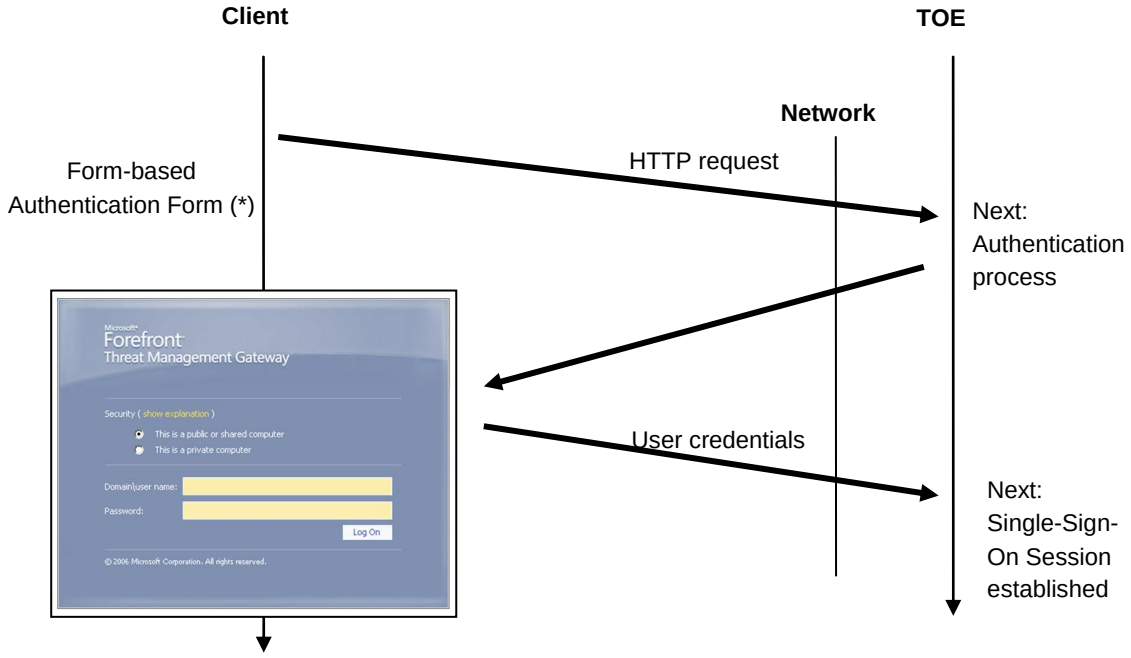
a) the underlying operating system (the OS verifies if the user credentials comply with the data stored in the local user database of Windows Server), or

b) a RADIUS server (the RADIUS Server verifies[9] if the provided user credentials comply with the data stored on the 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 7.2.1 “Web publishing”), when the user is allowed to access the internal resource. Additionally the TOE authenticates the user against the web application using HTTP Basic Authentication, so the client can access the resource without any additional authentication. The life-time of a Single-Sign-On Session is limited by:

- Time: the interval starting at the initial user sign-on and ending when the user is asked to enter credentials again.
- Client software: the client software that participates in the session. This spectrum reaches from a single browser window at one end to all client applications on the computer at the other end.
- Services: the services that the user can access (using client software) without being asked to re-enter credentials.

**Figure 7.2 – Web Identification & Authentication Process (Front-End Authentication)**




(*) symbolic photo showing the Form-based authentication form

[9] 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 7.3 – Web Identification & Authentication Process with local user database (Gateway Authentication with local user database)**

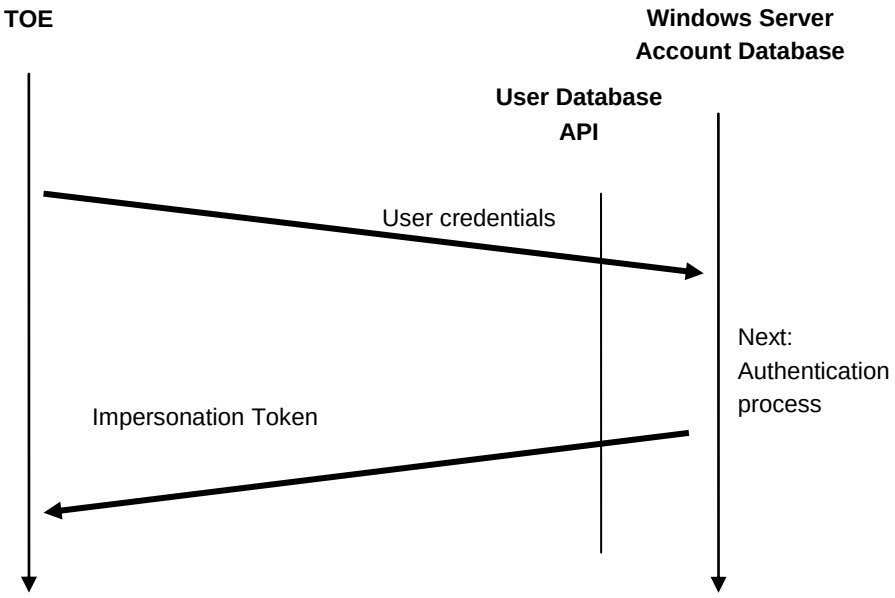



**Figure 7.4 – Web Identification & Authentication Process with Radius Server (Gateway Authentication, with Radius Server)**

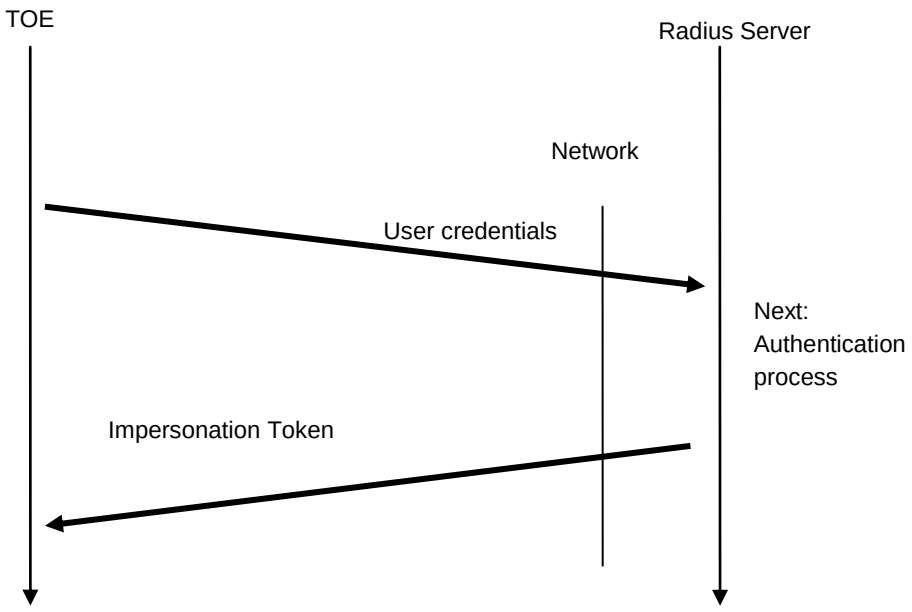
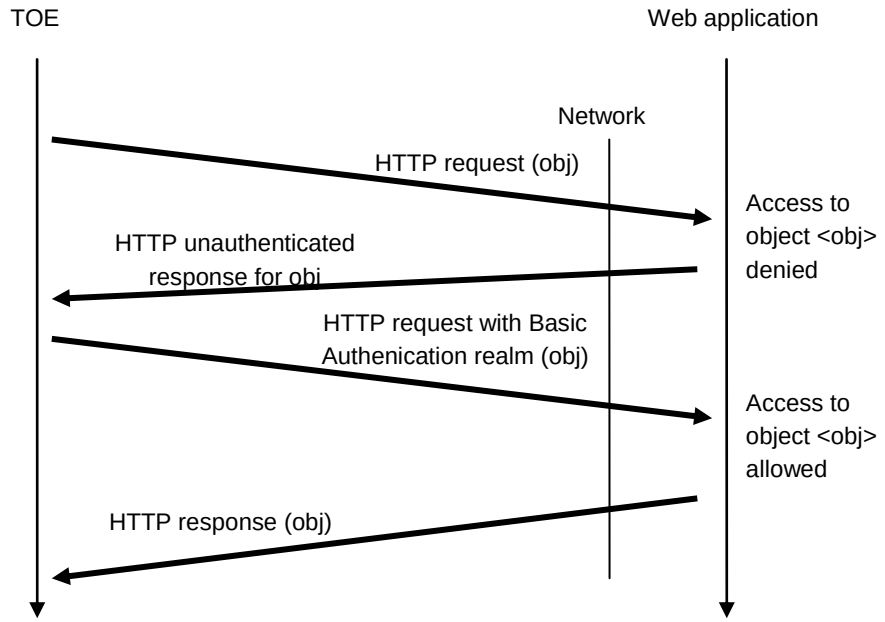


**Figure 7.5 – Web Identification & Authentication Process (Back-End Authentication)**




The following table comprises all possible combinations of Front-End, Gateway, and Back-End Authentication (combinations printed in bold are TOE related):

**Table 7.1 – Combinations of Front-End, Gateway, and Back-End Authentication**

| Front-End Authentication | Gateway Authentication | Back-End Authentication | Comments |
|---|---|---|---|
| **FBA (username, password)**<br>Basic | **Integrated**[10]<br>**RADIUS** | **Basic**<br>Integrated<br>TMG certificate | none |
| FBA (username, passcode) | SecurID | SecurID<br>Integrated<br>TMG certificate | * Applicable only if AD and SecurID usernames are the same (the administrator's responsibility). |
| FBA (username, password, passcode) | SecurID | SecurID<br>Basic *<br>Integrated *<br>TMG certificate | * Applicable only if AD and SecurID usernames are the same (the administrator's responsibility). |

[10] local Windows Server Account Database

| Front-End Authentication | Gateway Authentication | Back-End Authentication | Comments |
|---|---|---|---|
| SSL client certificate | AD-SSPI<br>TMG Internal | Integrated<br>TMG certificate | none |
| SSL client certificate + FBA (username, password)<br>SSL client certificate + Basic | AD-SSPI | Basic<br>Integrated<br>TMG certificate | none |

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

Related SFRs are: EXT_FIA_AFL.1, EXT_FIA_UAU.2, EXT_FIA_UID.2

## 7.2 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.

Related SFRs are: FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFC.1 (4), FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_IFF.1 (3), FDP_IFF.1 (4), FDP_RIP.1, FMT_MSA.3

### 7.2.1 Firewall Policy Rules

Firewall policy, which includes a set of publishing rules and access rules, together with network rules, determine how clients access resources across networks.

#### 7.2.1.1 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 7.2.2 for further details.

Related SFRs are: FDP_IFC.1 (1), FDP_IFF.1 (1), FDP_RIP.1, FMT_MSA.3

#### 7.2.1.2 Network rules (route and NAT)

It is possible to configure network rules in TMG, 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, TMG 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.

Related SFRs are: FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (2), FDP_IFF.1 (3)

#### 7.2.1.3 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 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.

Related SFRs are: FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (2), FDP_IFF.1 (3), FDP_RIP.1, FMT_MSA.3

#### 7.2.1.4 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 7.1).

Related SFRs are: FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (2), FDP_IFF.1 (3), FDP_RIP.1, FMT_MSA.3

Note:

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

### 7.2.2 Web filters

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

The “Form-based Authentication Filter” enables forms-based (cookie) authentication for publishing web applications like Outlook Web Access servers[11].

TMG can generate the forms used by Outlook Web Access and other web applications sites for forms-based authentication. This enhances security for remote access to these sites by preventing unauthenticated users from contacting the web application server.

The “Authentication Delegation Filter” allows delegating the authentication process. It can authenticate with the published servers, using the credentials provided by the user to the

[11] 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.

“Form-based authentication” filter. So a user can pass its credentials once and let TMG supply them to different published sites of the same domain without the need to retrieve the credentials several times from the client.

This functionality has been described in SF1: “Web Identification and Authentication” (chapter 7.1).

#### 7.2.2.1 URL filtering

URL filtering allows you to create access rules that allow or block access to Web sites based on their categorization in the URL filtering database. When a request to access a Web site is received, TMG queries the remotely hosted Microsoft Reputation Service to determine the categorization of the Web site. If the Web site has been categorized as a blocked URL category or category set, TMG blocks the request.

If a user requests access to a Web site and discovers that access to the Web site is blocked, he receives a denial notification that includes the denied request category. In some cases, the user may contact the administrator to dispute the categorization of the Web site. In such a case, the administrator must check that the URL was categorized properly (Looking up a URL category). If the Web site was not categorized correctly, then the administrator must manually re-define the category for this URL (override the default URL categorization).

Related SFRs are: FDP_IFC.1 (4), FDP_IFF.1 (4), FDP_RIP.1, FMT_MSA.3

### 7.2.3 Application filters

Application filters provide an extra layer of security at the Firewall service. Application filters can access the data stream 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.

Related SFRs are: FDP_IFC.1 (2), FDP_IFC.1 (3), FDP_IFF.1 (2), FDP_IFF.1 (3), FDP_RIP.1, FMT_MSA.3

#### 7.2.3.1 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 TMG 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).

#### 7.2.3.2 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.

#### 7.2.3.3 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.

### 7.2.4 System policy

TMG protects network resources, while connecting them securely for specifically defined needs. TMG introduces a system policy, a set of firewall policy rules that control how TMG computer enables the infrastructure necessary to manage network security and connectivity. TMG 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 TMG 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[12].

### 7.2.5 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[13]).

[12] Remote administration is not part of evaluation.

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

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 7.2.4) 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 SFP, FDP_IFC.1 (2) UNAUTHENTICATED_APPL SFP, FDP_IFC.1 (3) AUTHENTICATED SFP, FDP_IFF.1 (1) UNAUTHENTICATED SFP, FDP_IFF.1 (2) UNAUTHENTICATED_APPL SFP, and FDP_IFF.1 (3) AUTHENTICATED SFP, 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.

### 7.2.6 Policy Re-evaluation

Existing client connections will be reevaluated when the existing policy gets modified. Client connections not matching the newly enforced policy will be dropped.

This is handled with FDP_IFC.1 (1) UNAUTHENTICATED SFP, FDP_IFC.1 (2) UNAUTHENTICATED_APPL SFP, FDP_IFC.1 (3) AUTHENTICATED SFP, FDP_IFF.1 (1) UNAUTHENTICATED SFP, FDP_IFF.1 (2) UNAUTHENTICATED_APPL SFP, and FDP_IFF.1 (3) AUTHENTICATED SFP.

## 7.3 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

  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[14] using the MMC. Policy-change auditing allows to follow policy rules changes.

Related SFRs are: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.3

Note 1:

In Lockdown mode (see chapter 7.2.4) 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.

Note 3:

The TOE provides the ability to perform filter, search and sort operations on the recorded audit data. The selected, found or sorted data is displayed using the MMC.

## 7.4 Rationale on TOE summary specification

The specification of the TOE security functionality refers directly to the TOE security requirements. The following table displays the correlation between security requirements and security functionality.

[14] This includes several sorting and filtering features.

**Table 7.2 – Assignment of SFRs to security functionalities**

| # | 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_UAU.2 | X | | |
| 7 | EXT_FIA_UID.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_IFC.1 (4) – URL FILTER SFP | | X | |
| 12 | FDP_IFF.1 (1) – UNAUTHENTICATED SFP | | X | |
| 13 | FDP_IFF.1 (2) – UNAUTHENTICATED_APPL SFP | | X | |
| 14 | FDP_IFF.1 (3) – AUTHENTICATED SFP | | X | |
| 15 | FDP_IFF.1 (4) – URL FILTER SFP | | X | |
| 16 | FDP_RIP.1 | | X | |
| 17 | FMT_MSA.3 | | 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 using 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_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. The Form-based 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 which has to exist in the local user database to be authenticated successfully.

**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 Form-based 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 which 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

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

- UNAUTHENTICATED_APPL SFP

  The subjects under control of this policy are external IT entities on an internal or external network sending information on application level 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.

- URL FILTER SFP

  The subjects under control of this policy are external IT entities that send and receive HTTP(S) information through the TOE to one another on the result of a reputation service..

**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_IFC.1 (4)** (Subset information flow control (4)) is mapped to SF2 and identifies the entities involved in the URL FILTER information flow control SFP. It refers to the HTTP and HTTPS protocols used in Access rules that are used 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 and Mail publishing, Web publishing, Web and Application filters) 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 and Mail publishing, Web publishing, Web and Application filters) 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_IFF.1 (4)** (Simple security attributes (4)) is mapped to SF2 (Access Rules) and identifies the attributes of the information in the URL FILTER 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_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.

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.

# 8 Appendix

## 8.1 References


[CC] *Common Criteria for Information Technology Security Evaluation*, version 3.1, revision 3, July 2009
*Part 1: Introduction and general model,* CCMB-2009-07-001*,*
*Part 2: Security functional requirements,* CCMB-2009-07-002*,*
*Part 3: Security Assurance Requirements,* CCMB-2009-07-003

[MSTMG] *Microsoft Forefront TMG documentation – Standard Edition & Enterprise Edition,* Microsoft Corp.

[MSTMG_ADD] *Microsoft Forefront TMG Common Criteria Evaluation - Guidance Documentation Addendum,* Microsoft Corp.

[WEBTMG] Website: *Microsoft Forefront TMG - Common Criteria Evaluation*, http://go.microsoft.com/fwlink/?linkid=49507

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


## 8.2 Acronyms

| | |
|---|---|
| ADAM | Active Directory Application Mode |
| API | Application Programming Interface |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CC | Common Criteria |
| DLL | Dynamic Linked Library |
| EAL | Evaluation Assurance Level |
| EE | Enterprise Edition |
| FBA | Form-based authentication |
| FTP | File Transfer Protocol |
| GUI | Graphical User Interface |
| I & A | Identification and Authentication |
| ISA Server | Internet Security and Acceleration Server |
| IT | Information Technology |
| MMC | Microsoft Management Console |
| MRS | Microsoft Reputation Service |
| NAT | Network Address Translation |

| | |
|---|---|
| NIC | Network Interface Card |
| NLB | Network Load Balancing |
| OWA | Outlook Web Access |
| PP | Protection Profile |
| RAS | Remote Access Service |
| SE | Standard Edition |
| SF | Security Functionality |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SIP | Session Initiation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SPI | Stateful Packet Inspection |
| SQL | Standard Query Language |
| SSE | SQL Server Express |
| SSL | Secure Socket Layer |
| SSP | Security Support Providers |
| SSPI | Security Support Provider Interface |
| ST | Security Target |
| TLS | Transport Layer Security |
| TMG | Threat Management Gateway |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSP | TOE Security Policy |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |

## 8.3 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.<br>Active Directory Application Mode (ADAM) is a part of Microsoft's fully integrated directory services available with Windows Server, 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 data stream 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)] |
| 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. |
| datagram | In general, the term packet applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an "unreliable" service.[ |
| dynamic filters | Dynamic filters are automatically started by the Firewall service, Web proxy, or SOCKS proxy service. This feature allows the TMG services to automatically open and close communication ports on the external interface when transmission of packets is needed. |
| enterprise policy | Enterprise policy rules are applied to an array and used array wide. The effective array policy is the firewall behavior that results from the ordered set of rules that is the combination of the array-level and enterprise-level policy rules. Rules are processed in the following order: 1. Array-level system policy, 2. Pre-array enterprise rules, 3. Array-level firewall policy rules, 4. Post-array enterprise rules<br><br>For example, if an enterprise administrator wants to allow File Transfer Protocol (FTP) access across the enterprise without exception, a pre-array enterprise access rule allowing FTP should be created. However, if it is desired to allow FTP access but give the array administrators the ability to deny FTP access, a post-array enterprise access rule allowing FTP should be created. If an array administrator then creates an array access rule denying FTP, the effective policy will be that FTP is denied. If the array administrator does not create a rule that denies FTP, the effective policy will be that FTP is allowed. |

| | |
|---|---|
| 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 |
| Form-based authentication | Form-based authentication is a method of authenticating users using web-based forms for providing credentials. |
| 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 TMG, 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. |
| 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 | The Microsoft Management Console is a configuration management tool supplied with Windows that can be extended with snap-ins. The Microsoft Management Console – A configuration management tool supplied with Windows that can be extended with plugins. |
| MRS | The Microsoft Reputation Service (MRS) is a cloud-based object categorization system designed to provide comprehensive reputation content to enable core trust scenarios across Forefront and Microsoft security and management endpoint solutions. The first Forefront branded product that MRS will support is the Microsoft Forefront Threat Management Gateway (TMG). In the case of Forefront TMG, in order to find out the category of a URL, TMG issues an online query to MRS. MRS maintains a database with tens of millions of unique URLs and their respective categories. |
| MSP NAT Director | MS Proxy NAT Redirector |
| Network interface | A NIC or Network Interface Card is a circuit board or chip, which allows |

| | |
|---|---|
| card (NIC) | 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 Services, and others). This scheme is also sometimes referred to as the Windows NT Challenge/Response authentication scheme or Integrated Windows authentication. 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 TMG, either directly or indirectly, through a router. Clients can be configured either by using the Dynamic Host |

| | |
|---|---|
| | Configuration Protocol (DHCP) service or manually.<br><br>Strictly speaking SecureNAT clients are clients that are behind the firewall via Network Address Translation. Since TMG extends the network address translation (NAT) functionality, so all TMG rules can be applied to SecureNAT clients, and even though NAT does not have an inherent authentication mechanism, it is possible with TMG. 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. |
| Single-Sign-On | After providing the user credentials, the system issues a cookie, identifying the user. On subsequent requests, the system first checks the cookie to see if the user was already authenticated, so that the user does not have to supply credentials again. |
| 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 TMG 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 TMG. 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:<br>- Which Internet Protocol (IP) addresses and ports on the specified networks will listen for Web requests.<br>- Which authentication method will be used, when authentication is required.<br>- Number of connections that are allowed.<br>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 |