ATIS-1000046

ATIS Standard on -

DATA BORDER FUNCTIONS AND REQUIREMENTS

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Connected Vehicle, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit < http://www.atis.org >.

ATIS-1000046, *Data Border Functions and Requirements*

Is an ATIS Standard developed by the **Signalling, Architecture, and Control (SAC) Subcommittee** under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000046

ATIS Standard on

Data Border Functions and Requirements

Alliance for Telecommunications Industry Solutions

Approved August 2011

Abstract

This Technical Report (TR) defines the functions that are performed by, and the requirements for, the Data Border Function (DBF) within a Service Provider's network. Informative details on implementation realizations of a DBF are also provided. A DBF is comprised of a set of Session Security Functions together with Authentication and Proxy (A/P) functions. The separation of the DBF into its component functions is described, and session control, A/P, and OAM&P requirements are provided. In addition, the Data Border Function is mapped onto the Alliance for Telecommunications Industry Solutions (ATIS) Next Generation Network (NGN) Architecture (described in ATIS-1000018).

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Telcordia)

M. Dolly, PTSC-SAC Chair (AT&T)

S. Dawkins, PTSC-SAC Vice-Chair (Huawei)

J. McEachern, Technical Editor (Genband)

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

1 INTRODUCTION **1**

2 SCOPE, PURPOSE, AND APPLICATION **1**

3 REFERENCES **2**

3.1 ATIS REFERENCES 2
3.2 ITU-T REFERENCES 3
3.3 IETF REFERENCES 3
3.4 OTHER REFERENCES 3

4 DEFINITIONS **3**

5 ABBREVIATIONS **4**

6 DEPLOYMENT **6**

7 DBF FUNCTIONS **6**

8 DBF REQUIREMENTS **8**

8.1 GENERAL REQUIREMENTS 8
8.2 PERFORMANCE 9
8.3 SECURITY FUNCTIONS 10
8.4 AUTHENTICATION OF TRAFFIC FLOWS 12
8.5 PACKET MARKING 12
8.6 DEVICE OPERATIONS, ADMINISTRATION, MANAGEMENT AND PROVISIONING (OAM&P) 13
8.6.1 General Requirements 13
8.6.2 Alarms and Traps 13
8.6.3 Event Logging 14
8.6.4 Capacity Management 15
8.6.5 Performance Management 16
8.6.6 Provisioning/Configuration Management 16
8.7 DEVICE SECURITY 17
8.7.1 Cryptographic Certificates for Authentication 18
8.7.2 Session Security and Login Policy 18
8.7.3 Passwords 19
8.7.4 User Permissions 19
8.7.5 Application Administrator Permissions 20

9 COMPOSITION OF DBF **20**

A MAPPING TO ATIS NGN ARCHITECTURE **23**

TABLE OF FIGURES

FIGURE 1: DBF DEPLOYMENT EXAMPLE 6
FIGURE 2: DATA BE PROVIDING ALL SECURITY FUNCTIONS 21
FIGURE 3: AUTHENTICATION AND PROXY SERVICES LOCATED SEPARATELY FROM THE SECURITY FUNCTIONS 22

FIGURE A.1 : ATIS NGN HIGH-LEVEL ARCHITECTURE 23
FIGURE A.2: ATIS NGN FUNCTIONAL ARCHITECTURE SHOWING THE EAG 24

ATIS Standard on –

Data Border Functions and Requirements

1 INTRODUCTION

For session initiation and media transfer, secure access to the trusted elements of the Next Generation Network (NGN) is provided through a Session Border Controller (SBC) function that supports a number of security features, including protocol filtering and deep packet inspection, call admission control, and Internet Protocol (IP) proxy functions.

In addition to session initiation and media flows between end user devices, applications, and the service functions, there is a need for data flows for web-based services between the elements in the un-trusted domain and the elements in the trusted but vulnerable domain of the NGN. These flows are associated with actions such as call control via a WEB portal, downloading of device configuration information, accessing voice-mail from a third party server, and accessing authentication information from a different security domain. These flows will typically employ the use of "data" protocols such as HTTP, FTP, and Diameter -- which are not typically secured by a Session Border Controller function. This scenario primarily involves data protocols, but in some cases these flows will also include call control protocols such as SIP or Parlay-x when connecting to third party application providers.

Thus, there is a need for a function similar to that provided by the SBC, but in this case handling primarily data protocols. This function is referred to as the Data Border Function (DBF) in this Technical Report (TR).

2 SCOPE, PURPOSE, AND APPLICATION

This TR defines the DBF and the DBF requirements that are required to be performed within a Service Provider's network. The functions to be performed depend on the interface supported.

The following interfaces are supported from a Service Provider's network:

- To an Access Network
- To an Application Network
- To an Enterprise Network
- To a Residential Customer Network
- To a Transit Network
- To another Service Provider's Network

This TR defines the DBF and requirements for the above interface types. The physical realization of the functions will vary depending on implementations and deployments. The unification of these functions within a Data Border Element (DBE) and/or distribution of these functions over a number of DBEs will depend on scale, operational needs, and application needs.

The functions of the DBF include (but are not limited to):

- *Protocol Inspection*: Inspect incoming messages for supported protocols.
- *Intrusion Detection/Protection*: Provide Intrusion Detection/Prevention System (IDS/IPS) capability.
- *Stateful Firewall*: Provide a stateful firewall capability.
- *Authentication*: Provide authentication of connections before traffic is allowed into the trusted Data Network infrastructure.
- *Proxy*: Proxy all traffic to elements in the Trusted Domain.
- *Network Address Translation (NAT)*: Provide a NAT capability.
- *Traffic Policy Enforcement*: Limit excessive request volumes and excessive packet traffic.
- *Security Monitoring*: Monitor for unexpected, errored, and unauthorized messages, and respond appropriately for these messages.
- *Denial of Service (DoS) Attack Mitigation*: Provide functionality to mitigate DoS attacks.
- *Data Session Admission Control*: Provide admission control for selected data traffic.
- *DSCP Packet Marking*: Ensure packets have the correct DSCP markings.

The main sections of the document are:

- Section 6 (*Deployment)* defines logical relationships between elements in the trusted and un-trusted network domains.
- Section 7 (*DBF Functions)* defines the functions of the DBF in detail.
- Section 8 (*DBF Requirements)* defines the detailed requirements on the functions independent of the physical realization.
- Section 9 (*Composition) of DBF* describes implementation options.
- Appendix A (*Mapping to ATIS NGN Architecture)* identifies the architecture functional entities that perform DBF functions.

3 REFERENCES

3.1 ATIS References[1]

[T1.TR.70-2001] *A Reliability/Availability Framework for IP-Based Networks and Services*(2001)

[ATIS-0100016] *E2E Service Availability: General Definition* (2007).

[ATIS-0100020.2008] *Quantifying Impact on IP Service Availability from Network Element Outages* (2008).

[ATIS-0100025] *Methodology for Estimating Access IP Router Availability in Terms of Customer Facing Line Card Availability* (2009).

[ATIS-0100028] *Network Resiliency Planning for Enterprise Customers* (2010).

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[ATIS-0100524.2004 (R2008)] *Reliability Related Metrics and Terminology for Network Elements in Evolving Communications Networks* (2004).

[ATIS-1000018] *NGN Architecture* (2007).

[ATIS-1000029.2008] *NGN Security Requirements* (2008).

3.2 ITU-T References[2]

[M.60] ITU-T M.60, *Maintenance: Introduction and General Principles of Maintenance and Maintenance Organization*, March 1993.

3.3 IETF References[3]

[RFC 2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., "Hypertext Transfer Protocol – HTTP/1.1", RFC 2616, IETF, June 1999.

[RFC 2818] Rescorla, E., "HTTP Over TLS", RFC 2818, IETF, May 2000.

[RFC 4252] Ylonen, T., Lonvick, C., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, IETF, May 2006.

[RFC 3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J., "Diameter Base Protocol", RFC 3588, IETF, September, 2003.

[RFC 5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, IETF, October, 2008.

[RFC 959] Postel, J., Reynolds, J., "File Transfer Protocol (FTP)", RFC 959, IETF, October, 1985.

[RFC 1350] Sollins, K., "The FTTP Protocol (Revision 2)", RFC 1350, IETF, July, 1992.

[RFC 792] Postel, J., "Internet Control Message Protocol", RFC 792, IETF, September, 1981.

[RFC 5905] Mills, D., Martin, J., Burbank, J., Kasch, W., "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, IETF, June, 2010.

[RFC 1035] Mockapetris, P., "Domain Names – Implementation and Specification", RFC 1035, IETF, November, 1987.

[RFC 5424] Gerhards, R., "The Syslog Protocol", RFC 5424, IETF, March, 2009.

[RFC 2714] Ryan, V., Seligman, S., "The Syslog Protocol", RFC 5424, IETF, October, 1999.

3.4 Other References

[i3 Forum] i3 Forum White Paper, "Security for IP Interconnections (Release 1.0)", June 2011.[4]

4 DEFINITIONS

4.1 Data Border Element: A physical realization of a DBF or portions of a DBF.

---

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[4] This document is available at < http://www.i3forum.org/library >.

4.2 Data Border Function: The set of functions that enables interactive communication for data flows across the borders or boundaries of different IP-based networks.

NOTE: A DBF provides access control and security for interactions which employ standard data protocols such as HTTP, FTP, and Diameter.

4.3 Denial of Service (DoS): 1. The prevention of authorized access to resources or the delaying of time-critical operations. 2. The result of any action or series of actions that prevents any part of an information system from functioning.

4.4 DoS attempt: A malicious attempt to overload a network element, or network elements, in a manner such that it cannot perform its intended function.

4.5 Firewall: A system designed to protect a computer network from unauthorized access, especially via the Internet.

4.6 Network Address and Port Translation: Network Address and Port Translation (NAPT) is a method of converting one IP address space and port number to another IP address space and port number.

4.7 Network Address Translation: Network Address Translation (NAT) is a method of converting one IP address space to another IP address space.

4.8 Network to Network Interface (NNI): The control and media interface between two networks, used to provide connectivity to other NGNs, other IP-based networks, or the PSTN.

4.9 User to Network Interface (UNI): UNI is the interface between a UE and a service provider network, including all protocol levels.

4.10 Network footprint scan: A technique of gathering information about computer systems and the networks that connect them by employing various techniques, such as DNS queries and port scanning.

4.11 OS finger print scan: The passive collection of configuration attributes from a remote device during standard layer 4 network communications, to infer the remote machine's operating system (OS) by taking advantage of the fact that certain parameters within the TCP protocol definition are left up to the implementation. Also known as *TCP/IP stack fingerprinting***.**

4.12 Traceroute: A computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

5 ABBREVIATIONS

This document uses the following abbreviations:

AAA	Authentication, Authorization, and Accounting
A/P	Authentication and Proxy
AS	Application Server
ATIS	Alliance for Telecommunications Industry Solutions
CIDR	Classless Inter-Domain Routing
DBE	Data Border Element
DBF	Data Border Function
DDoS	Distributed Denial of Service

DNS	Domain Name System
DoS	Denial of Service
EAG	External Application Gateway
EMS	Element Management System
FCAPS	Fault-management, Configuration, Accounting, Performance, Security
FTP	File Transfer Protocol
GUI	Graphical User Interface
GW	Gateway
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
MIB	Management Information Block
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NGN	Next Generation Network
NNI	Network to Network Interface
NTP	Network Time Protocol
OAM&P	Operations, Administration, Maintenance, and Provisioning
OSS	Operations Support System
PAM	Pluggable Authentication Modules
PCI	Peripheral Component Interconnect
RFC	Request for Comments
RPH	Resource Priority Header
SAC	Session Admission Control
SBC	Session Border Controller
SCP	Secure Copy Protocol
SIP	Session Initiation Protocol
SNMP	Service Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial FTP
TLS	Transport Layer Security
TTL	Time to live

UNI	User to Network Interface

6 DEPLOYMENT

Figure 1 shows the DBF in the context of the security trust model defined in [ATIS-10000029], where the DBF is a border element that enables secure communication between an un-trusted domain and a trusted network domain.

The Data Border Function enables secure communication between an un-trusted domain and a trusted domain. There are several possible end point types in the un-trusted domain that may need to communicate with the elements in the trusted domain. These end point types include End User devices, Enterprise networks, 3rd party Application Servers (AS), and gateways (GW) to other networks.

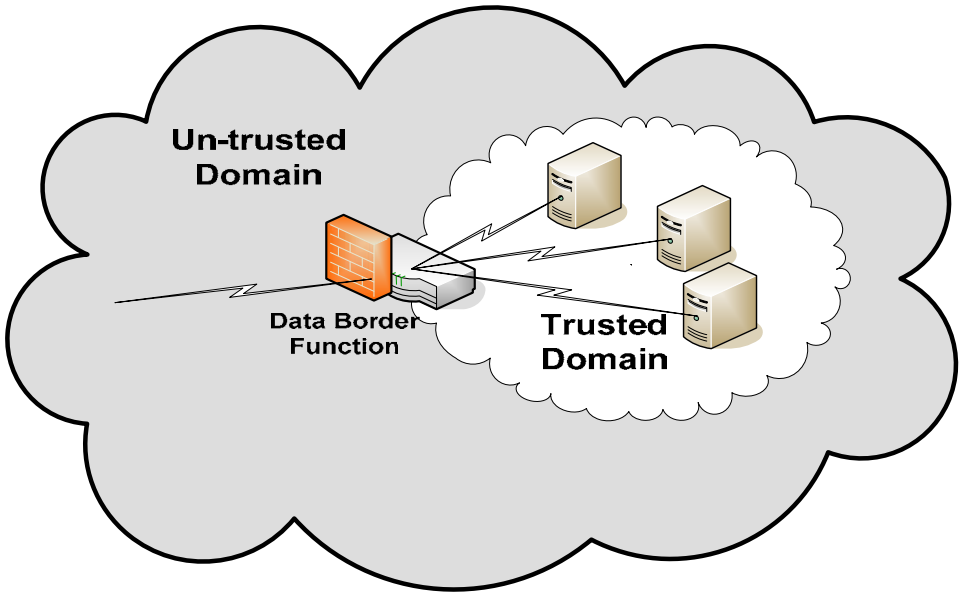

Figure 1: DBF Deployment Example

7 DBF FUNCTIONS

The following functions shall be supported by the DBF:

- *Encrypted Traffic*: If an incoming traffic flow is encrypted, the DBF shall decrypt the traffic if it has the key, and apply applicable policies. The DBF shall have the corresponding capability to encrypt outgoing traffic, depending on applicable policy. If the DBF does not have the key to decrypt encrypted traffic, it shall have the ability to either drop the traffic, or pass it transparently, depending on applicable policy.

- *Protocol Inspection*: For each protocol supported, stateful inspection of the incoming message shall be performed to ensure that it conforms to the protocol specification. If there is an error in the message, the DBF should -- if possible -- repair the message. If this is not possible, the packet(s) should be dropped and an error logged.
- *Intrusion Detection/Protection*: The DBF shall support Intrusion Detection/Prevention System (IDS/IPS) capabilities. For example, the DBF shall support the capability to inspect the payload for embedded malware. It shall be possible to update the detection "signatures" that use an algorithm employing "bit pattern search and matching" to accomplish "look ups" in a single CPU cycle to identify and terminate second attempts as new vulnerabilities are identified. A flexible policy definition capability shall be available to specify the actions that shall be taken in terms of inspection, and the disposition of packets that pass/fail inspection.
- *Stateful Firewall*: The DBF shall support firewall capabilities for which rule sets can be defined to control the traffic flowing between un-trusted and trusted domains.
- *Authentication*: All connections into the trusted network domain shall first be authenticated by the DBF. Since the specific authentication requirements are application dependant, there will be an application specific component of the DBF. Several authentication mechanisms are acceptable including username/password, HTTP challenge/response, mutual certificate authentication, etc. Selection of the authentication method(s) to be applied will be based on the assurance level needed for the specific data application.
- *Proxy*: All traffic passing into the trusted domain from an un-trusted domain shall be proxied. In many cases, this function will require application knowledge and thus the proxy function may be included in the implementation of the Authentication function
- *NAT*: The DBF shall support NAT (NAPT) capabilities to "hide" the location of elements within the trusted domain. It shall be possible to perform NAT on both source and destination addresses. In some cases, the specific NATing requirements may be application-dependent, and so it shall be allowable for the application specific function of the DBF to perform the NATing function. It shall also be available as a common function of the DBF.
- *Traffic Policy Enforcement*: The DBF shall have the capability to limit excessive requests and excessive packet traffic.
- *Security Monitoring*: The DBF shall have the capability to recognize and, based on policy, drop packets in a flow that do not conform to the protocol being used for that flow. For example, the DBF function shall be able to recognize packets that appear out of sequence, incomplete packets, and packets indicating a different protocol and shall be able to drop these packets.

  The DBF shall have the capability to drop packets from flows when the packets are associated with a protocol that is not supported.
- *DoS and Distributed Denial of Service (DDoS) Attack Mitigation*: The DBF shall employ mechanisms such as the use of White lists/Black lists and Media Pin Holing to detect and mitigate DoS and DDoS attacks. Load balancing/clustering capabilities with the DBF should also be available to provide sufficient system scale to absorb attacks, as well as a flexible detection system to analyze attacks, and the capability to interact with cleaning systems that can use the results of analysis to remove attack traffic before it reaches targeted network elements.
- *Data Session Admission Control (SAC)*: The DBF shall implement admission control mechanisms based on definable policies.

- *DSCP Marking*: The DBF shall provide a mechanism for modification of the DSCP markings on incoming packets and marking outgoing packets based on definable policies. The policies shall be definable on a per flow basis.

8 DBF REQUIREMENTS

This section defines specific requirements associated with the functions of the DBF. The DBF may be implemented using several physically separate units. In the following requirements, a requirement associated with a "DBE" is applicable to each physical unit making up the solution. Requirements referring to the DBF relate to the whole integrated solution.

NOTE: In this section, the term "user" refers to an administrator or craftsperson. It does not refer to an end user.

8.1 General Requirements

The Data Border Element (DBE) shall support the capability of defining multiple virtual instances within one physical implementation. Virtual instances of the DBF behave as if they were separate physical devices, even though they are running on a single physical device.

Each virtual instance shall have a distinct enforcement policy associated with it.

The DBF shall have the ability to Proxy traffic on all IP Flows.

The DBF shall have the capability of performing Network Address Translation (NAT) and Network Address and Port Translation (NAPT) on IP Flows.

The Proxy and NAT functions shall be uniquely configurable for each "virtual instance" of the DBF.

The DBF shall be capable of performing "policy enforced rate limiting" on a per IP flow basis.

The DBF shall support the capability of being able to separate traffic destinations by using methods other than multiple IP addresses such as higher layer header information, or port numbers, thereby limiting the number of addresses required to be allocated for the DBE trusted and un-trusted interfaces.

The DBF shall support more than one IP address (from different IP address blocks) on the un-trusted and trusted sides.

The DBF shall support Internet Protocol Security (IPSec) and Transport Layer Security (TLS) tunnel terminations.

The DBF shall have support for "ping" functionality. DBEs should be configurable so that they do not respond to "ping" and thus can be "invisible" on the network.

The DBF shall support traceroute functionality.

The DBF shall be able to perform Domain Name System (DNS) lookups.

The DBF shall support policy objects created by Classless Inter-Domain Routing (CIDR) block segmentation.

The DBF shall support access to multiple Network Time Protocol (NTP) servers to maintain accurate timing for log collections.

The DBF shall at peak operation (i.e., peak line rate on all interfaces concurrently); continue to support management functions; and remain available, operational, and functional.

The DBF shall support the ability to initiate Transmission Control Protocol (TCP) reset, or Internet Control Message Protocol (ICMP) unreachable packets.

A DBE shall add less than a millisecond of latency regardless of policy, utilization, or packet profile. This time does not include any delays due to accessing external systems such a DNS.

Unless dictated by security policies in place, the DBE shall maintain no packet loss, at line rate, and under a variety of packet size profiles.

8.2 Performance

This section describes the computing platform, availability, performance and physical implementation requirements for the DBF. If the DBF is implemented in more than one physical unit (DBE), these requirements apply to each physical unit (DBE). Applicable performance specifications can be found in T1.TR.70-2001, *A Reliability/Availability Framework for IP-Based Networks and Services*, and ATIS-0100524.2004 (R2008), *Reliability Related Metrics and Terminology for Network Elements in Evolving Communications Networks*.

> **"Availability"** is the percentage of time the system is capable of being used. It is calculated using the entire system's mean time between failures (MTBF) and the mean time to repair (MTTR): Availability = MTBF / (MTBF + MTTR). Availability can also be represented by the number of minutes a system is down per year excluding scheduled maintenance periods.

The DBF shall be at least 99.99% available. This equates to less than 52 minutes of unscheduled downtime per year. This applies to all Fault-management, Configuration, Accounting, Performance, Security (FCAPS) functionality combined. As an objective, any individual DBE should be at least 99.999% available.

Each DBF shall be at least 99.99% available. This equates to less than 1 failure in 10,000 FCAPS tasks. As an objective, the DBE shall be at least 99.999% reliable.

The DBF shall incorporate built-in mechanisms for process throttling for session management, memory allocation, and CPU utilization for state and sessions to mitigate the impact of contention and prevent exhaustion of resources for both dynamic and static processes within the device.

The DBF shall support the option of using active/active high availability configuration with state transference, or active/hot standby high availability configuration with state transference.

The DBF shall support Fail OPEN forwarding after sudden device failure, within 50 milliseconds.

The DBF shall support automatic IP packet re-route after link failure.

The DBF should support the use of a M:N high availability.

Overload conditions shall not cause the complete failure of the DBF. Overload shall only result in a graceful degradation of the system platform performance. The DBF shall discard packets in order to avoid a complete system failure.

The DBF shall provide interface and session level statistics gathering and display ability, with configurable resets.

8.3 Security Functions

The DBF shall be capable of enforcing security policies.

The DBF shall support the ability to enforce security policy that was in effect prior to any interruption in power subsequent to the power being restored.

The DBF shall support automatic session termination when it determines that packets associated with that session are anomalous. The automatic session termination can be controlled by design or by configurable policy.

The DBF shall treat all packets that it identifies as DoS/DDoS packets (inbound and outbound) according to network provider policy (e.g., drop packets, or direct packets to specific network security services).

The DBF shall attempt to splice TCP sessions based on information obtained during the TCP handshake with the intention of validating that the initiator of the proposed TCP conversation is offering a valid session. If it is deemed that it is not a valid session, the DBF shall drop the session and log the event.

The DBF shall support stateful analysis and retention of state for IP flows through the DBF. Stateful analysis is important to identify security threats.

The DBF shall support "application layer" awareness to the extent that it shall inspect and verify L4-L7 protocols for specific application use in accordance with the applicable IETF-Request for Comments (RFCs) for the protocol. Specific protocols to be supported shall include, but are not limited to:

a. HTTP
b. HTTPS
c. SSH
d. Diameter
e. SMTP mail protocols outbound
f. TFTP, FTP
g. ICMP
h. NTP
i. SCP
j. DNS
k. SYSLOG
l. IIOP
m. SIP
n. Parlay-x

The DBF shall support the ability to drop packets with TTL=0/1.

The DBF shall detect and report network footprint scans by design or policy.

The DBF shall detect and report system finger print scans by design or policy.

The DBF shall support the use of thresholds for security events to minimize false positives and adjust for baseline conditions.

The use of global rules shall be supported in the configuration of the firewall.

The DBF shall include the configurable ability to explicitly log application of the "implicit deny" rule associated with every policy. (Note: at the end of every list of allowed actions, there is an implicit rule to deny anything that is not explicitly allowed by the rules. When this "implicit deny" is used to block traffic, it shall be possible to log this.)

The DBF shall provide detection and policy enforcement functionality using vulnerability-based signatures.

The DBF shall support performing deep packet inspection L4-L7 -- based on policy -- while inspecting packet payload for malicious traffic, and shall perform this with no packet loss and no increase in latency or jitter. Should packets containing malicious traffic be detected, they shall be treated according to the applicable security policy (e.g., dropped and a security log generated).

The DBF shall provide policy enforcement functionality for tunneled applications (unencrypted).

The DBF shall support the detection of security threats encapsulated in another service or standard protocol (e.g., packets being carried through an unencrypted IPSec tunnel).

The DBF shall support the detection and policy enforcement functionality using a statistical protocol or application analysis engine that is preconfigured for common attacks and fully configurable for user defined attack type threshold detection settings.

The DBF shall support attack detection based on signature pattern matching.

The DBF shall support the capability of disabling the Intrusion Prevention System (IPS) capabilities of a single virtual instance through configuration parameters.

It shall not be possible to change the configuration of the IPS capability for a DBF virtual instance "on the fly", but shall require the instance to be shut down, re-configured, and brought back up in the new configuration.

The DBF shall be able to report on intrusion detection results (successful, blocked, suspicion, etc.), and capture and analyze all information related to a potential intrusion -- including packet logs.

The DBF shall be capable of performing deep packet analysis of at least the following protocols:

a. HTTP
b. HTTPS
c. SSH
d. Diameter
e. SMTP mail protocols outbound
f. TFTP, FTP
g. ICMP
h. NTP
i. SCP
j. DNS

k. SYSLOG

l. IIOP

m. SIP

n. Parlay-x

The DBE shall provide detection and policy enforcement functionality using defined signatures.

The DBF shall support the capability to receive updated signatures.

It shall be possible to selectively configure each device, signature, policy, or filter for mitigation or monitor mode.

The DBF shall have the ability to switch its Intrusion Detection capability from passive tap mode to active inline protection mode within seconds, without physical intervention on a per port basis and with no increase in latency.

The DBF shall support the application of local policy or filters based on IP options.

8.4 Authentication of Traffic Flows

The DBF shall support authentication of sessions being established through the DBE.

Authentication shall be configurable on each physical and logical interface on the "un-trusted" side of the DBF.

For authentication of sessions being established through the DBF, the authentication mechanism for each session should be based on the assurance level needed for the specific data application. For example:

a. Username/Password

b. Challenge/Response (e.g., HTTP MD5 Hash)

c. Mutual Certificate authentication

Authentication may be performed by the DBF itself, or the authentication request may be directed to an associated authentication server such as an Authentication, Authorization, and Accounting (AAA) server.

As a configurable option, the DBF shall be able to block traffic for any unauthorized data flow.

8.5 Packet Marking

The DBF shall support DSCP Packet Marking for packets flowing from the trusted domain to the un-trusted domain based on policies configurable for each flow or based on a global default policy.

The DBF shall support inspection of DSCP packet marking on packets flowing from the un-trusted domain to the trusted domain, and shall have the capability of changing the marking based on policies configurable for each flow or based on a global default policy.

8.6 Device Operations, Administration, Management and Provisioning (OAM&P)

8.6.1 General Requirements

An Element Management System (EMS) is required to manage the DBF solution. If the DBF solution is realized using several integrated components, the EMS shall provide an integrated view of all components.

The EMS system shall be capable of managing multiple instances of the DBF.

The DBF shall respond to "ping" on the Management Interface.

DBE shall provide the capability, both locally and remotely through the EMS, to change the operational state of a component or resource.

A Service Network Management Protocol (SNMP) Management Information Block (MIB) that represents the characteristics of the DBF hardware platform shall be provided.

If applicable, an SNMP MIB that represents the characteristics of the operating system supporting the DBF applications shall be provided.

8.6.2 Alarms and Traps

The DBF shall have the ability to send traps to the EMS and also to a separate interface to an upstream OSS system.

The DBF shall be capable of generating a heartbeat in the form of an SNMP trap every x minutes, where x is a configurable integer parameter, and send it to the alarm monitoring system.

A set of measurements shall be provided to support fault management and maintenance functions. These shall include element-level and resource-level measurements as well as link/data-link measurements.

DBF shall provide thresholding of measurement data to configurable values. When these measurements exceed the threshold value, the DBE detecting the event will generate an alarm indication with a unique trap ID. For example, if available local disk storage is < 20%, then that DFE shall generate a unique trap.

A DBF shall provide the ability to assign a severity level to specific alarms through a management interface.

When failures in a DBF affect the ability for an element to receive/process signaling messages, the element shall have the ability to detect this condition and turn off the affected resources. Transactions in progress should be allowed to complete if possible. This condition should be reported to the local console, EMS, and remote interface (OSS) via an alarm with a unique trap ID.

A DBF shall identify and report alarms related to its internal interfaces, external interfaces (e.g., remote nodes), and remote interfaces (i.e., OSS).

The DBF shall be able to send unique traps to multiple, configurable destinations (usually the EMSs will be one set of destinations and one or more OSSs will be the other destinations for any particular traps).

Fault monitoring shall be configurable to generate unique alarm/trap IDs, and send them to the EMS and remote interface (i.e., OSS). Examples include, but are not necessarily limited to:

a. *CPU*: Utilization, errors, core dumps.

b. *Temperature*: Die and/or ambient.

c. *Fans*: Individual fans, fan tray, fan speed.

d. *Memory*: Utilization, faults.

e. *Disks*: Utilization, errors, thrashing, busy, queue length.

f. *Field Replaceable Units (FRUs)*: Health, redundancy state change.

g. *Power Supply*: Individual supplies, power bus inputs, voltage levels, current levels.

h. *System*: Cold start, warm start, panic.

i. *Processors*: Errors, inactive.

j. *Peripheral Component Interconnect (PCI)*: Link up/down, retransmissions, network collisions, packet loss, protocol errors.

k. *Hardware Down/Up*.

l. *Operating System* (memory, file systems, etc).

m. *Application Monitoring* (log file, process, etc.).

n. *Database Monitoring*.

o. *System Monitoring* (log files, process, etc).

p. *Intersystem Connectivity*.

Configurable thresholds shall be supported for generating operating system resource usage traps.

Configurable severity levels shall be supported for generating operating system resource usage traps.

For initial hardware installation and whenever hardware is grown (e.g., a plug-in card is added), the system shall verify that the added hardware module matches the type of hardware for which the system is configured. All errors shall generate SNMP traps and debug logs.

For initial hardware installation and whenever hardware is grown (e.g., a plug-in card is added), the system shall run self-diagnostics and generate success or failure SNMP traps and debug logs.

8.6.3 Event Logging

The DBF shall support the use of multiple SYSLOG servers for policy enforcement action logs.

The DBF shall use role-based management for authentication/authorization of event viewing and forensic data analysis to control access to log data.

The DBF shall provide a capability to log:

a. All permitted inbound access requests from network clients that use a service identified in the security policy hosted on the device or protected network segment.

b. All permitted outbound access requests from the protected network segments that use a service identified in the security policy to access a network server

c. All access requests inbound or outbound that are intended to traverse the device and, which if they did, would violate the security policy

d. All access requests from any client that attempts to send traffic to the device (DBF) itself, which if it did, would violate the security policy.

e. All attempts to authenticate on the administrative interface.

f. All access requests from any client that attempts to send traffic to the device on ports reserved for remote administration.

The DBE shall provide certain required log data including (but not necessarily limited to):

a. Date and Time format (DD/MM/YYYY, HH:MM:SS)

b. Protocol from the IP Header

c. Source IP Address

d. Destination IP Address

e. Source Port

f. Destination Port

g. Message Type (if ICMP)

h. Disposition of Event

i. Success/Failure to authenticate on the Admin interface with supporting reason.

All required log data corresponding to all required log events shall be available for review upon demand and presented in a human readable format while preserving the relative timing sequence of events.

The DBF shall support the ability to retain log events, that have not been sent to a log server during a power outage, and retain those logs unaltered for transport after power is reapplied.

8.6.4 Capacity Management

The DBF shall have the ability to monitor the following capacity indicators:

- IP traffic data
- Link Utilization
- CPU utilization

DBE shall provide time interval traffic measurement data, where the specific interval is configurable (e.g., 15 minutes or 30 minutes). This data will be used for capacity planning and shall be able to be sent to the EMS and/or an upstream OSS.

All measurements of throughput, lost/dropped packets, and link utilization shall include separate counts for each direction of transport at each relevant interface.

IP traffic data shall be collected in time intervals, and for each functional element the following information shall captured or created: packet throughput, average and peak buffer utilization, packets dropped and packets lost, and link utilization.

Capacity measurement data shall be accessible through the EMS via a Graphical User Interface (GUI) interface.

Capacity measurement data shall be able to be retrieved by an upstream OSS on-demand, and shall be able to be reported automatically according to a configurable schedule.

8.6.5 Performance Management

The DBF shall monitor the following performance indicators, including (but not necessarily limited to):

- Link utilization
- CPU utilization

The DBF shall provide time interval measurements (e.g., 5-minute), on-occurrence event indications, and controls to allow monitoring the performance of the solution and the network and to apply controls as appropriate in cases of congestion or network events, such as natural disasters or mass calling events. These should include the statistics, notifications, and controls related to all protocol layers.

Measurements shall be provided on intra-node delay, throughput, packet loss, and connectivity for network elements and interfaces in the IP network.

Each functional element of the DBF solution shall provide measurements of CPU utilization and on-occurrence overload indicators related to system operation.

DBF shall provide time interval traffic measurement data. These measurements may be used for Network Management, and shall be able to be sent to the EMS and/or an upstream OSS.

All measurements of throughput, lost/dropped packets, and link utilization shall include separate counts for each direction of transport at each relevant interface.

IP traffic data shall be collected in time intervals, and for each DBE shall include packet throughput, average and peak buffer utilization, frequency of buffer overflow, packets dropped and packets lost, and shall include link utilization. The counts shall be collected for each direction of the transport separately,

Performance measurement data shall be able to be retrieved by an upstream OSS on-demand, and shall be able to be reported automatically according to a configurable schedule.

8.6.6 Provisioning/Configuration Management

Each element of the DBF solution shall support electronic updates of its generic software.

Each element of the DBF solution shall maintain a record of its current software version

Activation of the software shall be possible via the local console, EMS, and the remote interface (i.e., OSS).

The Generic update process for a functional element shall complete within a specified length of time, and in the event of an unsuccessful generic upgrade load, back-out procedures shall also be completed within a time period no longer than the update time.

A mechanism shall be provided to ensure the integrity of upgrade files before application.

In the event of an unsuccessful generic upgrade load, back-out procedures and capabilities shall be available. A mechanism shall be provided to soak an upgraded functional element before committing to the SW upgrade.

Configuration data, Database and Software Back-up, and Restore capabilities shall be supported.

Safe stop points shall be provided in the upgrade process.

The EMS shall be able to support a network with DFBs running different generics. At least two generics shall be supported for each DBF vendor.

The DBF shall support scheduling capabilities for applying software updates.

Bulk download of configuration information to each set of functional elements shall be supported remotely through the EMS. Configuration data is data that is the same in each element -- e.g., office parameters.

Tools shall be provided to identify and correct data inconsistencies.

It shall be possible for each of the elements in the DBF to be configurable locally via the console, and remotely through the EMS using its GUI.

If applicable, the solution shall support the provisioning of all solution functional elements through the EMS by a user and by upstream OSS(s) connected to the EMS.

All provisioning inputs shall be acknowledged with either success or failure, and in case of failure, a reason shall be provided. In case of errors or failures, the user shall be able to determine the status of the order (e.g., in case of partial failure).

The users shall be able to query the DBF for values of provisioned data elements.

It shall be possible to configure the DBF to send notifications to a remote OSS whenever the value of a user specified set of data elements is changed. It shall be possible to specify which data elements changes lead to notifications and which remote OSS system(s) will receive the notifications. This capability allows the OSS view of the provisioned data and that of the solution to be consistent.

8.7 Device Security

The DBF shall allow all unused Operating System services to be disabled, and all unused ports to be closed.

The DBF shall have a means of providing a secure remote login.

The DBF shall not have any processes which require that applications shall run with root privileges.

The DBF shall support use of trusted time sources.

The DBF shall maintain an audit of security relevant events and be able to detect and alarm on attempted modification of the audit trail.

The DBF shall have a means of securely sending log files to remote hosts.

The DBF shall have a means of sending security alarms on the OAM&P interface.

All OAM&P interfaces shall be secured per requirements in [ATIS-1000029].

8.7.1 Cryptographic Certificates for Authentication

It is desired that remotely interconnecting components shall authenticate with each other using a cryptographic certificate based mechanism.

8.7.2 Session Security and Login Policy

- *Login Display Message*: Each system component shall be able to display a message configurable by the network administration to warn all users of the consequences of non-authorized use of the system prior to the login process. If telnet or ftp or other access methods are supported, the DBE shall also enable a warning message display during login processes for these access methods.
- *User Authentication*: Each system component shall authenticate all users before granting them access to the system, including those users that access the system using the GUI client, telnet, ftp, etc. (e.g., by requiring them to enter a user ID and password).
- *Scripting of Logins*: Each system component shall prohibit the scripting of login mechanisms. Human users shall be forced to manually enter their credentials each time they log in.
- *Requests and Operations*: Each system component shall be able to associate each request or operation with a unique user ID so that it may be properly authenticated and logged.
- *Freezing of User Accounts*: Each system component shall support freezing a user account after a fixed number of unsuccessful login attempts. This number shall be settable with a default setting of five attempts. When the user account is frozen, the DBE shall not identify this as the reason for unsuccessful login to the user.
- *Unsuccessful Login Attempts*: Each system component shall log unsuccessful login attempts and the freezing of a user's account due to too many unsuccessful login attempts.
- *Security Notification*: Each system component shall generate a security notification in response to freezing a user's account due to too many unsuccessful login attempts.
- *Display of Last Date and Time*: After a successful login, the system component shall display the last valid login date/time and number of unsuccessful attempts since then made with that user's ID.
- *Simultaneous Sessions*: Each system component shall be able to limit the simultaneous use on multiple sessions of the same user id. The number of simultaneous active sessions shall be settable per user id with a default value of one.
- *Inactive Session Timeout*: Each system component shall support inactive session time-outs. A user's session shall automatically be locked after a period of inactivity. This period shall be configurable (with a default value of 15 minutes). Once a user's session is locked, the DBE shall force the user to re-authenticate before continuing the session.
- *Inactivity Timeouts*: In addition to normal logins and logouts, inactivity session timeouts shall also be recorded in the session accounting logs.

- *Explicit Logout*: Each system component shall provide a means for the user to explicitly logout, thus ending that session for that authenticated user and recording the end of the session in session accounting logs.
- *Expired Accounts*: Each system component shall automatically disable the accounts of users that have not logged in for a long period of time. This period of time shall be settable for each user, with a default setting of 30 days.
- *Security Bypass*: There shall be no mode of entry into the application software for maintenance, support, or operations that will violate or bypass the security procedures.
- *Security Violation Alarms*: Each system component shall provide a security alarm notification in the event of detection of attempted DBE security violations.
- *Security Violation Logging*: Each system component shall log attempted security violations.

8.7.3 Passwords

Password requirements for the DBF shall be based on network security policy. The security features of the DBF should take into account the following factors:

- Password encryption and display.
- Rules and restrictions for password construction.
- Rules for when passwords must be changed.
- Rules for password reuse.
- Rules for password/user removal.

8.7.4 User Permissions

- *Unique User Identity*: Each system element shall allow each user to have a unique identity within the system.
- *User Authorization*: Each system component shall ensure that each user performs only authorized functions and accesses only the authorized resources.
- *Access Permissions*: Each system component shall support three levels of access permission to resources:
    1. No access;
    2. Read only; and
    3. Read-write.
- *User Profiles*: Each system component shall allow the configuration of different DBE user profiles (or groups) that define the functions a user is authorized to perform, and allow these profiles to be assigned to users. There shall be no arbitrary limitation on the number of user profiles.
- *User Profile Authorizations*: Each system component shall enable the definition of user profiles with authorizations based on network resource information, including:
    1. Networks (all of the nodes and links contained by a network).

2. Nodes and the access links that terminate on them.
3. Ports.
4. Customer data, if any.

- *User Profile Functional Authorizations*: Each system component shall enable the definition of user profiles with authorizations based on function type (e.g., configuring nodes, provisioning services, viewing faults, and administering the network element server application).

8.7.5 Application Administrator Permissions

The ability to administer each system component application shall be included in user profiles. Users authorized to perform this function are referred to as "Application Administrators" in this document. The DBF shall not allow any user without administrator privileges to execute programs on the DBF.

- *"Root" Authorization*: No system component shall require an Application Administrator to be a system administrator or "root" user at the operating system level of the server.
- *Multiple User IDs for Administators*: Each system component shall allow multiple user IDs to be authorized to perform application administrator functions.
- *Minimum Administrator Authorization*: Each system component shall ensure that at least one user is authorized to perform application administrator functions.
- *Administrator Functions*: Each system component shall enable an application administrator (and only an application administrator) to:
  - Create, modify or delete DBE application user identifications.
  - Reset passwords.
  - Set password expiries, inactivity timeouts and allowed password re-try attempts.
  - Create, display, modify, or delete DBE user profiles.
  - Assign user profiles to user IDs.
- *User Termination*: Each system component shall allow an application administrator to terminate any active user or system session.
- *User Session Termination*: When a user ID is deactivated by an application administrator, each system component shall automatically terminate any active sessions associated with that user ID in a timely fashion.
- *"Raw" Capability Access*: Access to the raw capabilities of the underlying System server operating system (e.g., file system access and "shell" or command prompt access) shall be granted only to system component users that are specifically authorized to do so in their user profile or to users that use some other means besides the system component application (e.g., telnet) to access the platform. Note that the application need not enable any users to access the server operating system, but if it does, it shall only allow those specifically authorized to do so.

9 COMPOSITION OF DBF

The DBF may be implemented as a single physical entity or the various functions may be implemented in separate physical devices. This results in a number of possible deployment scenarios for the DBF.

The following figures illustrate two possible alternative deployments. The first (Figure 2) shows the DBF providing all the border element functions in a single location, whereas Figure 3 illustrates a situation where the Authentication and Proxy functions are provided by an application server "in front" of the Firewall/IPS security functions. In this latter case, the Application Server itself is protected from the un-trusted domain by a firewall, and the interface between the Auth/Proxy functions and DBF is a secure connection, such as an IPSec tunnel or dedicated facility. The area between the un-trusted and trusted domain is considered to be "trusted but vulnerable" since it is has been authenticated, but does not have the full protection offered by the DBF.

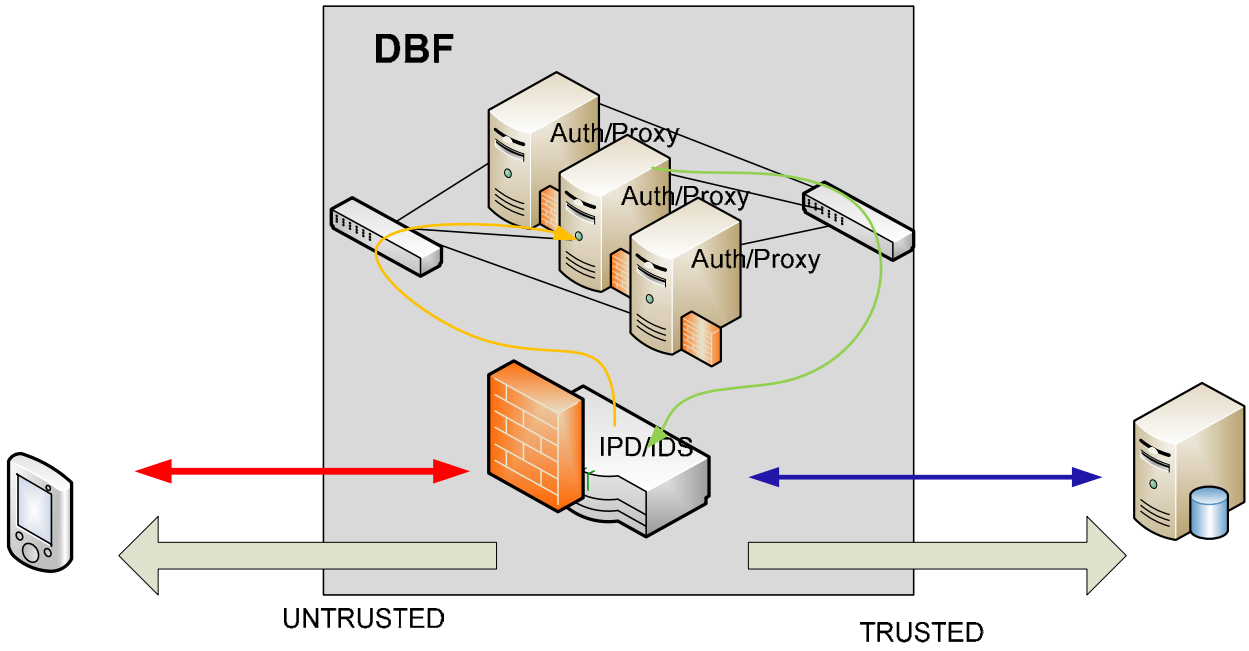

Figure 2: Data BE Providing all security functions

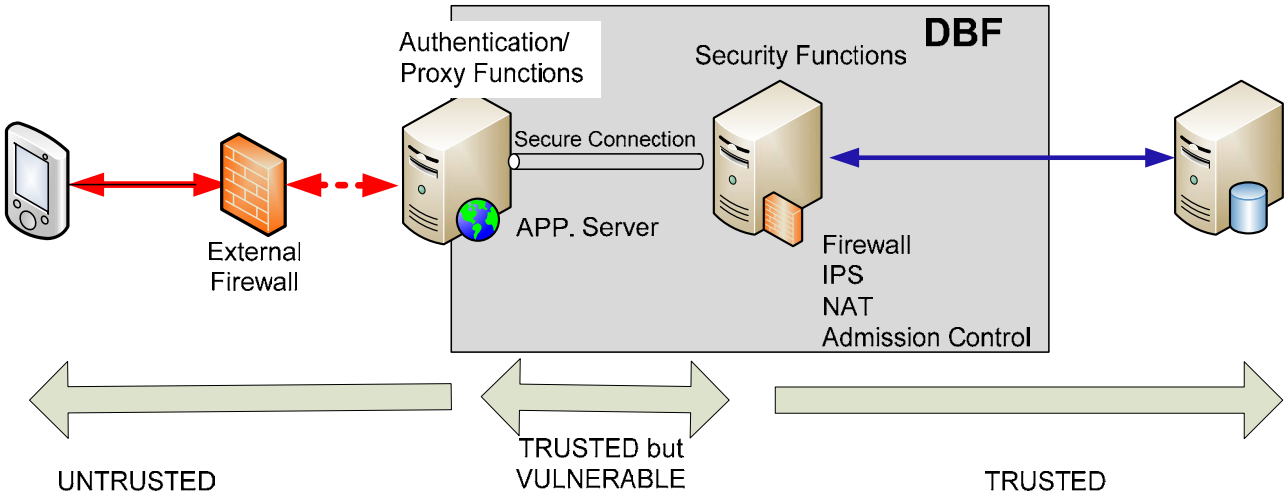

Figure 3: Authentication and Proxy services located separately from the Security functions

Appendix A

A MAPPING TO ATIS NGN ARCHITECTURE

The following diagram shows the ATIS high level NGN architecture.

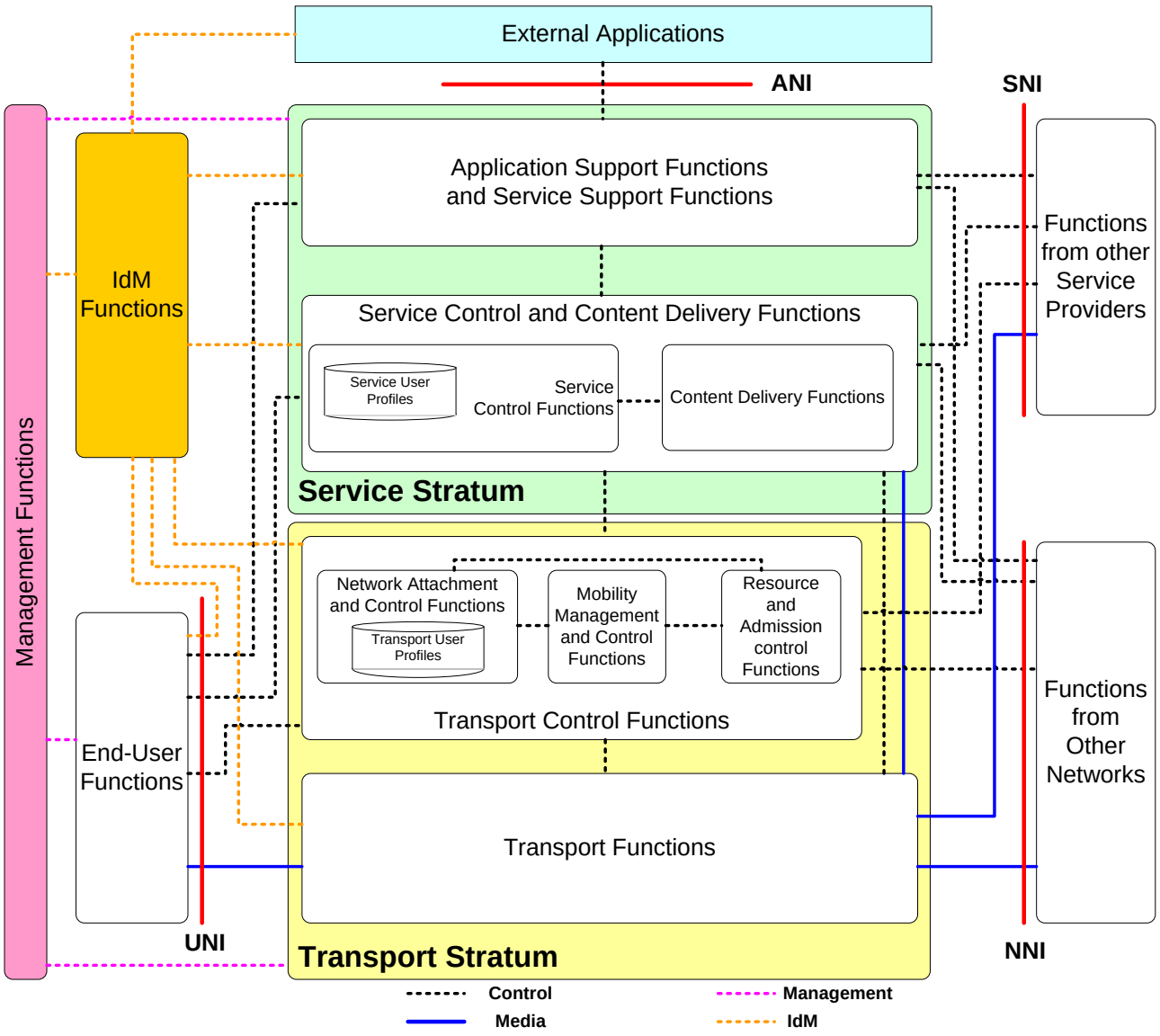

Figure A.1 : ATIS NGN High-level Architecture

Within the context of this architecture, the DBF controls access to the trusted NGN for all untrusted sources. The protocols the DBF handles will typically be "data" protocols, although in the case of untrusted third party application providers, this could also include call control protocols such as SIP or Parlay-x. These protocols could be used to remotely access voicemail, initiate voice calls from a web page, or authenticate a UE from the un-trusted Internet. Within the NGN, these interfaces will

generally terminate in the NGN Service Stratum, but in the un-trusted domain they could terminate on an application server, an un-trusted network, or a UE. The interface to the DBF is similar to the ANI in the NGN architecture except for the protocols it handles. The protocols across the ANI could be SIP or an API such as Parlay-x, while the DBF typically deals with "data" protocols such as HTTP, FTP, and Diameter. The DBF is in the "Application Support Functions and Service Support Functions" block in the NGN architecture.

The DBF must also be considered in the context of the ATIS NGN Functional Architecture, as shown below. The ATIS NGN architecture includes an External Application Gateway (EAG) that allows the user to access web based services in the NGN from other application or Service Providers. The DBF can provide the EAG and WSG functions shown in this architecture. The following diagram shows the EAG (DBF) positioned within the ATIS NGN functional architecture.

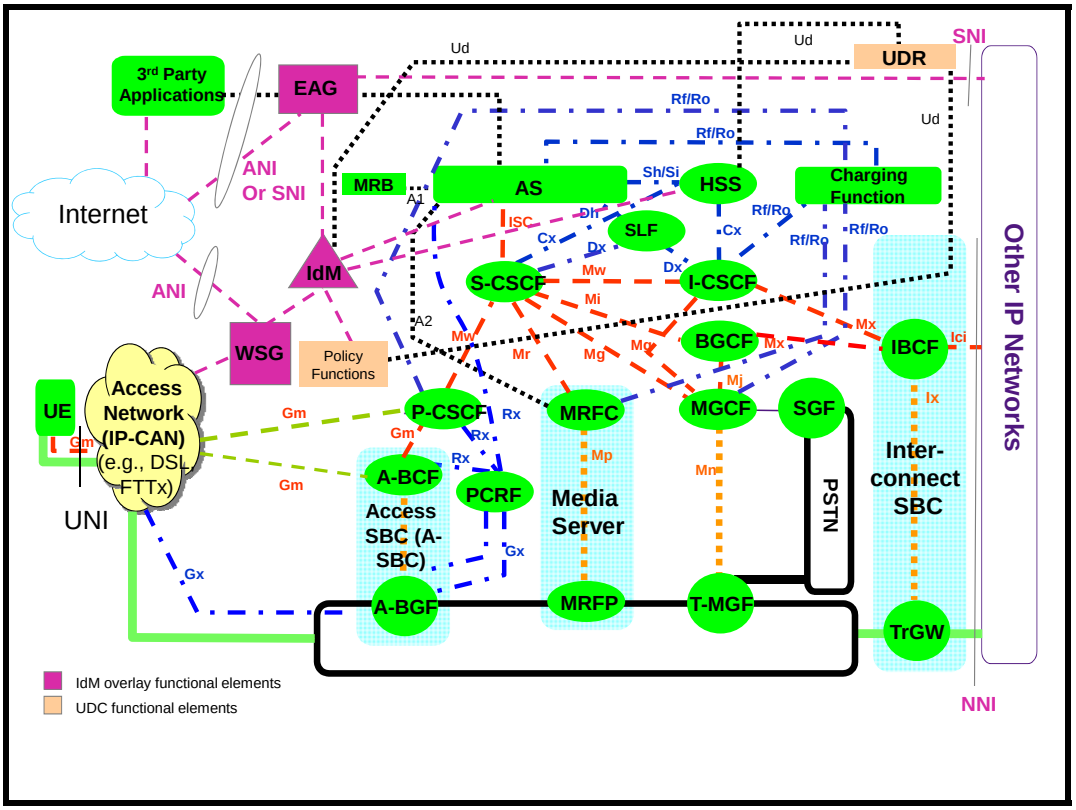

Figure A.2: ATIS NGN Functional Architecture showing the EAG