ETSI TS 187 021 V3.2.1 (2014-04)

Security services and mechanisms for customer premises networks connected to NGN

Reference
RTS/NTECH-00009-SEC-CPN

Keywords
gateway, IP, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Network Technologies (NTECH).

1 Scope

The present document specifies the functional models and information flows (stage 2) and protocols (stage 3) which implement the security services and mechanisms required to provide security in a Customer Premises Network (CPN) to support the overall security architecture for NGN release 3. CPN security services and mechanisms are used either singly or in combination to realize the CPN security requirements specified in TS 187 001 [1] (NGN Security requirements). Reference will be made to TR 185 012 [i.1] for security mechanisms that have been shown to be appropriate for CPN environment.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[2] ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

[3] ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points".

[4] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[5] Broadband Forum TR-069 Amendment 3: "CPE WAN Management Protocol", November 2010.

[6] Broadband Forum TR-157 Amendment 3: "Component Objects for CWMP", November 2010.

[7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 185 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) Feasibility study of security mechanisms for customer premises networks connected to TISPAN NGN".

[i.2] IETF RFC 5209 (June 2008): "Network Endpoint Assessment (NEA): Overview and Requirements".

[i.3] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

[i.4] ETSI TS 102 825 (all parts): "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)".

[i.5] ETSI TS 183 065: "Telecommunications and Internet converged Services and Protocols for Advanced Networks(TISPAN); Customer Network Gateway Configuration Function; e3 Interface based upon CWMP".

[i.6] Broadband Forum TR-069: "CPE WAN Management Protocol".

[i.7] IEEE 802.16: "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems".

[i.8] IEEE 802.1b: "IEEE Standard for Local and Metropolitan Area Networks - Local and Metropolitan Area Network: LAN/MAN Management".

[i.9] Home Gateway Initiative: "Home Gateway Technical Requirements V.1.0".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 187 003 [4] and Broadband Forum TR-157 [6] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACS	Auto-Configuration Server
AKA	Authentication and Key Agreement
ALG	Application Level Gateway
API	Application programming Interface
B2BUA	Back to back User Agent
BGF	Border Gateway Function
BL1	Boot Loader image
CA	Conditional Access
C-BGF	Core- Border Gateway Function
CND	Customer Network Device
CND-CMF	CND-Configuration and Management Function
CND-CPF	CND-Content Protection Function
CND-CSMF	CND-Communication Service Media Function
CND-SPF	CND-Service protection Function
CNG	Customer Network Gateway
CP	Content Protection
CPE	Consumer Premise Equipment
CPN	Customer Premises Network
CW	Control Words
DLNA	Digital Living Network Alliance
DMZ	DeMilitarized Zone
DOS	Denial Of Service
DRM	Digital Right Management
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
DVB-CPCM	DVB Content Protection & Copy Management
FW	FirmWare
HGI	Home Gateway Initiative
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem

IPSEC	Internet Protocol SECurity
IPTV SP	IPTV Service Provider
IPTV	Internet Protocol TeleVision
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
MCF	Media Control Function
MDF	Media Delivery Function
MF	Media Function
MFC	Media Control Function
NAC	Network Access Control
NAT	Network Address Translation
NEA	Network Endpoint Assessment
OMA	Open Mobile Alliance
PAT	Port Address Translation
PC	Protection Client
PCL	Protection Client Loader
PCO	Protection Client Owner
P-CSCF	Proxy-Call Session Control Function
PDA	Personal digital assistant
PPP	Point to Point Protocol
QoS	Quality of Service
ROM	Read Only Memory
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SMS	Short Message Service
SOC	Security-on-Chip
SP	Service Protection
SP/CP	Service Protection and/or Content Protection
SSL	Secure Socket Layer
STB	Set Top Box
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UC	Unsolicited Communication
UDP	Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTM	Unified Threat Management
VOD	Video On Demand
VPN	Virtual Private Network
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WPA2	Wi-Fi Protected Access 2

4 General overview

This clause introduces the subset of security mechanisms to be evaluated and specified in details within the present document. The security mechanisms has been selected mainly (but not only) from the contents of the TR 185 012 [i.1].

5 Firewalling

The main mechanism to perform Network Access Control is a firewall, i.e. a system designed to permit, deny or proxy data traffic to or from the customer's network. A firewall is positioned to control all incoming and outgoing traffic; hence the CNG is the perfect candidate to perform the firewall functions.

5.1 Firewalling: basic description

There are several approaches to implements firewall functionalities, such as:

- Packet Filtering: the simplest one inspects each incoming or outgoing IP packet permitting, dropping or rejecting it on the basis of simple policies (usually defined as access control list) such as the IP address and the protocol type.
- Stateful Firewall: in addition to a Packet Filter, keeps track on IP packets belonging to the same connection thereby detecting whether a packet is part of an existing connection or a start of a new connection.
- Application Level Gateway: In addition to a stateful firewall can understand the behaviour of some applications and can detect e.g. if an illegal protocol is used for a given application or dynamically open ports for additional sessions belonging to a flow.

Firewalls can divide the network into subnets each one with a different level of security and different security policy as for example a demilitarized zone.

The firewall could have several configuration alternatives:

- A basic/minimum configuration to ensure a minimum level of security.
- One or several default configurations provided and managed by the operator/service provider through a remote management system.
- Additional alternative configurations that can depend on the user (e.g. there can be different configurations for parents and children). These user specific configurations could be managed by the same entity managing the user identity (e.g. the UICC).

5.2 Firewalling: architecture

In the CPN context, the CNG sits between the NGN and the internal network and this aspect makes the CNG as the perfect candidate to host the firewall functions. Figure 1 shows a typical scenario where the CNG and the Firewall are co-located on the same device. The external interface is the one that is connected to the NGN via e.g. xDSL, IEEE 802.16 [i.7] wireless modem, FTTx, etc., and is often referred to as the unsecure (red) interface. The secure (black) internal interfaces are connected to the CNDs and can be based on ethernet, IEEE 802.1b [i.8] and other wired or wireless communication technologies. The firewall may also implement a DMZ.

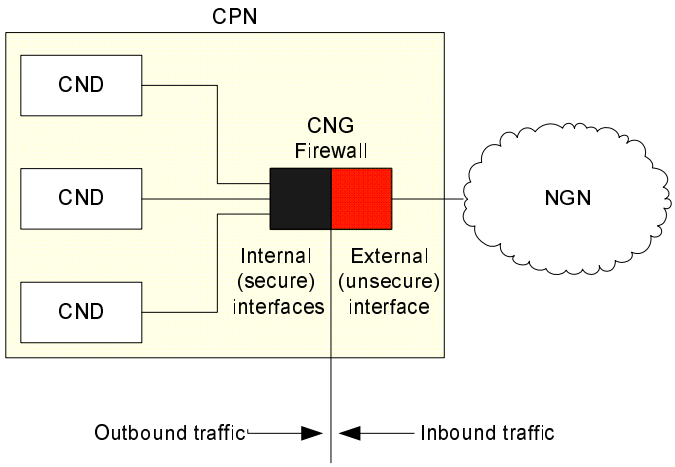

Figure 1: Firewall in the CPN

The advantages of using a Firewall as shown in the picture (i.e. co-located on the CNG) is that the CNG appears to the external network (i.e. NGN) as the only point of contact for the CPN, simplifying the protection of the CNDs against threats that originate on the NGN.

5.3 Firewalling: implementation details

For the protection of the CPN, a firewall should support some basic features, such as security policy definition and enforcing, firewall management, logging functions and so on. The following clause describes in details such features.

5.3.1 Stateful inspection

The stateful firewall function is mandatory for the protection of the CPN, such a firewall function may be implemented in the CNG. While a packet filter decides whether or not to drop a packet based on few information contained in the packet headers (e.g. addressing information), a stateful packet filter takes its decisions also on the state information that the firewall keeps in memory about all active connections travelling across it.

For connection-oriented protocols, such as TCP, the state of the connection is equivalent to the protocols definition of a connection (i.e. three-way handshake), whereas for a connection-less protocol, such as UDP, the state of the connection is the set of packets that are sent between common endpoints (i.e. source IP address/port and destination IP address/port) without interruption, i.e. the lack of any packets matching that flow for a given period of time. For the CPN context such a period of time shall be one minute.

The stateful firewall shall also perform additional structural checks on network packets. These checks include e.g. quickly dropping of malformed packet and enforcing the TCP three-way handshake to establish and teardown network connections.

5.3.2 Communication technologies

The Firewall shall be enabled on the local CPN network including all kind of wired and wireless connectivity used on the CPN, as well as remote access connections such as PPP over Ethernet and Virtual Private Network on the WAN side of the CNG. Note however that the firewall cannot be enabled when the CNG acts as a network bridge.

IPv6 firewalling shall be implemented in case the CNG supports IPv6 traffic.

5.3.3 Security policy

The firewall could have several configuration alternatives. In order to simplify the management of the security policy and still provide a basic level of security to the CPN it is proposed to define one or more security profiles.

As defined by HGI in [i.9] at least the following basic configurations shall be supported by the firewall: *HIGH* security configuration and *LOW* security configuration.

The *HIGH* security configuration foresees the following behaviour:

- For the traffic originated from the NGN toward the CPN (inbound): to refuse connections in TCP, UDP and ICMP; to authorize already established connections only (and known by the stateful firewall).
  Based on the Operator/Service Provider local policy, the firewall could accept incoming connections for specific services/ports, such as 5 060 for SIP (e.g. inbound SIP calls).

- For the traffic originated from the CPN toward the NGN (outbound): to authorize only well known ports, such as:

  - 25 - SMTP
  - 80 - HTTP
  - 443 - SSL
  - 554 - RTSP
  - 995 - POP3
  - 123 - NTP
  - 5 060 - SIP

A second alternative basic firewall configuration shall be supported by the firewall, the *LOW* security configuration: all traffic (inbound and outbound) is authorized by default. Anyway the stateful firewall still performs the security check on the TCP/UDP active sessions.

Also Internet Control Message Protocol (ICMP) messages should be managed because these messages can be used in hacking and DOS attacks. The firewall should block or allow specific ICMP options (e.g. Echo Requests, destination unreachable).

Additional alternative configurations can depend on the user preferences and/or Operator/Service Provider local policy.

5.3.4 ALG for standard protocols support

Also a stateful firewall is not effective or could limit specific services with applications that include IP addresses and TCP/UDP port information in the payload (e.g. FTP, SIP protocols, peer to peer applications). To filter these protocols, and at the same time permit the access to such services, the firewall has to be augmented by specific Application Level Gateway.

The firewall should contain support for the NGN standard protocols, such as SIP and RTSP, for the pinholing of the media ports so that the inbound and outbound traffic could flow through the CNG.

Note that when B2BUA is implemented inside the CNG, TS 185 003 [3], it acts as a SIP ALG; in this case the B2BUA shall interact with the firewall.

5.3.5 Firewall management

The firewall should be manageable from the CPN and by the IPS/Operator and it should enable the ISP/Operator also to upgrade the firewall functionality via download of a new configuration file. To implement this operation, the management centre downloads to the CNG firewall the configuration file. This file integrates the basic firewall configuration that includes the HIGH and LOW configurations. As described by HGI in [i.9], DSL Forum TR-069 [i.6] provides mechanisms for configuration file downloads. The CPN firewall should support TR-069 [i.6]. However, some additional mechanisms and specifications could be needed to fully support the CPN security requirements, for example OMA device management which supports also the security of the management.

The management features should permit the upgrade of the software firewall, the management of the security policy and the access to the logging information.

5.3.6 Logging

The firewall should have the ability to log network traffic and main security events. Basic logging options should be supported (by default all logging options should be disabled). The logging function should capture at least the following events:

- Log of changes to firewall policy.
- Network connection logs, which include dropped and rejected connections (for both inbound and outbound packets).
- Log of software firewall upgrade events.

The log files should be accessible from the remote management.

6 SP and/or CP secure upgrade

6.1 SP and/or CP secure upgrade: introduction and scope

6.1.1 Introduction

Interoperability of the CPE (IPTV CND or CNG) means that the end user can switch the CPE to another IPTV service provider without having to change the CPE (assuming that the transmission technology does not change).

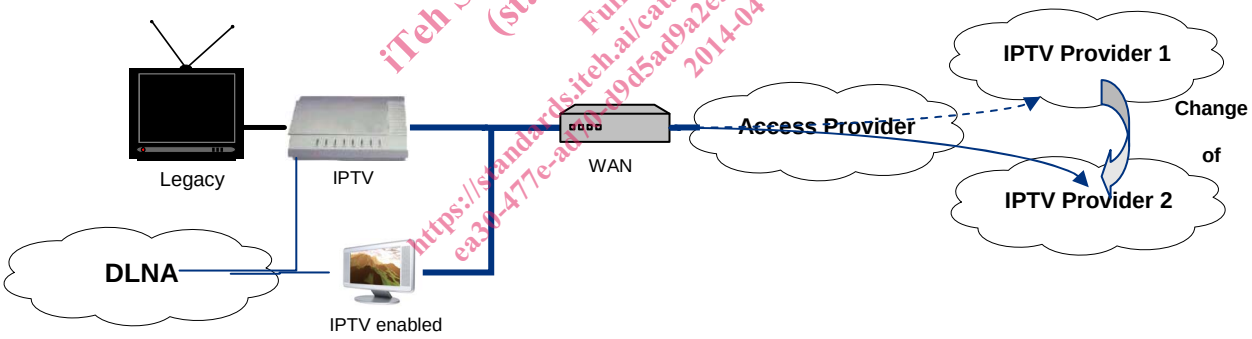

Figure 2: SP & CP architecture

An IPTV specific requirement which has a strong influence on interoperability is the use of service and/or content protection (SP/CP) systems aka CA/DRM systems.

Service Protection/Content Protection Interoperability (in short SP/CP Interoperability) of CPE with a IPTV Service Providers offering means that an end user can switch to another Service Provider (using a different SP/CP system) to obtain service from whilst retaining his CPE equipment.

In order for CPE not to have to implement every (possibly proprietary) SP/CP system that exists, for such kind of interoperability CPE is required to support upgrade/renewal of its SP/CP software and potentially the cryptographic algorithms used by the SP/CP system for scrambling content.

NOTE 1: This type of interoperability does not solve the reuse of previously bought protected content, when the SP/CP system changes. Frameworks like DVB-CPCM (see all parts of TS 102 825 [i.4]) solve that inter CP interoperability problem on the CPE side, this is also an important topic but it is complementary to the CPE - service provider interoperability addressed in this clause.

NOTE 2: Once a SP/CP software is upgraded and taken into operation there is no further dependency on the SP/CP upgrade mechanism.