International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1011
(10/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – General security aspects

Guidelines for continuous protection of the service access process

Recommendation ITU-T X.1011

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	**X.1000–X.1029**
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1011

Guidelines for continuous protection of the service access process

Summary

The prevention of unauthorized access to information and abuse of information and communication technology (ICT) resources is fundamental to cybersecurity. An extensive effort had been made towards the standardization of identity and access management. However, the access environment is continuously changing and traditional mechanisms are unable to deal with the challenges of evolving security threats. This is firstly because traditional data centre infrastructure is moving to the cloud, and consequently the perimeter security devices for traditional data centres are not applicable to cloud-based data centres. Secondly, internal threats are becoming more and more serious, e.g., authorized users trying to perform dangerous operations caused by negligence, or internal users being attacked by social engineering which may lead to impersonation risks. Thirdly, the status of user devices or resources may become insecure during the access process, e.g., operating system (OS) or software in user devices and resource platforms being compromised by exploitation of misconfigurations, or access requests being intercepted, etc.

The service access process is the process during the interval between a subject (i.e., user and user device) initiating access request(s) and receiving response(s) from a service, which may involve a variety of the above-mentioned security threats.

In order to deal with these challenges, it is crucial to continuously analyse related security status, verify the rationality of access activity, protect the security of access processes and prevent unsecure access. Recommendation ITU-T X.1011 defines a reference framework for keeping continuous protection of the service access process.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1011	2021-10-29	17	11.1002/1000/14793

Keywords

Access process, continuous security, reference framework

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1011

Guidelines for continuous protection of the service access process

1 Scope

This Recommendation analyses security threats to the service access process, specifies security protection measures to detect abnormal access activities and introduces an enhanced authorization mechanism for service access. This Recommendation includes the following:

- Analysis of security threats and challenges in the service access process;
- Specification of security requirements of the service access process; and,
- A reference framework to mitigate identified threats thus keeping continuous protection of the service access process.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.1252]: A procedure by which an administrator can restrict access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 authentication [b-ITU-T X.1252]: Formalized process of verification that, if successful, results in an authenticated identity for an entity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights and, based on these rights, the granting of access.

3.1.4 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in context.

NOTE 1 – An entity can have a physical or logical embodiment.

NOTE 2 – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, and interfaces.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 continuous protection: A security protection process to lessen the security risk of an object in as timely a manner as possible, including the following activities: continuous hardening of all its associated systems, detecting insecure entities and behaviors, dynamically enforcing authorization decisions and responding to threats.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABAC	Attribute Based Access Control
ACL	Access Control List
DDoS	Distributed Denial of Service
DoS	Denial of Service
EDR	Endpoint Detection and Response
ICT	Information and Communication Technology
IMS	Identity Management System
IP	Internet Protocol
OS	Operating System
P2P	Peer to Peer
RBAC	Role Based Access Control
MITM	Man-in-the-Middle
SDCD	Security Data Collection and Detection
SDK	Software Development Kit
TIS	Threat Intelligence Service
VPN	Virtual Private Network
ZT	Zero Trust

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Security threats of the service access process

6.1 Insufficiency of perimeter-based security mechanism

Along with the development of digitalization, more and more enterprises are providing services online. At the same time the deployment environment of enterprise services is moving from traditional data centres to cloud-based services. A service may frequently use some cloud-based resources external to an enterprise's network. Therefore, the physical perimeter of networks is disappearing, and consequently traditional perimeter-based security mechanisms (e.g., deployment of security equipment at network perimeter, etc.) are no longer applicable or feasible.

6.2 Risk of exposing services

Direct exposure of a service's processes/resources internal to an enterprise to the user via the Internet may profoundly increase the attack surface, e.g., denial of service (DoS) attacks, port scanning, etc.

6.3 Risk of unknown devices

Employees and partners may use unknown user devices which are not controlled by the enterprise to access a service. These unknown user devices bring uncertainty to security.

6.4 Internal threat

An unintentional or malicious activity made by a careless or malicious employee could cause significant threat to an enterprise. An attacker may intrude into the enterprise's Intranet by stealing credentials of normal users. Consequently internal entities of an enterprise are not always trustful.

6.5 Privilege abuse

Traditional access authorization decisions depend on user roles and static attributes (e.g., access time, physical network location, protocol type, etc.), and often provide a coarse-grained network-level and application-level authorization. The coarse-grained access control policy may not provide enough security protection for services in time, and potentially there may be privilege abuse attacks.

6.6 Leakage of sensitive information about access requests

The attacker may launch a man-in-the-middle (MITM) attack to obtain the sensitive information such as user credentials and business data via the communications between the subject (i.e., user and user device) and the service.

7 Security requirements of the service access process

The security requirements of the service access process are as follows:

– It is required that all the requests are authenticated and authorized before being granted to access. This means the subject that initiates the request should have an independent identity and be treated as one entity when accessing, which can reduce the risk of stolen user credentials or user devices.

– It is recommended that all the services are not directly exposed to the user via the Internet, so that services are protected from being discovered as targets by attackers.

– It is recommended that all communications between the subject and services are encrypted to maintain the confidentiality and integrity. This will help to avoid interception and tampering with communication data by attackers.

– It is recommended that access control is dynamic, and the decision is not two-value (granted or not granted). A subject that is authorized to access a service at one time does not mean that the subject will have the access privilege all the time. It is recommended to degrade a subject's privilege (for example from writing to reading privilege) when the subject is not as secure as previously.

– It is recommended that all the user devices that may initiate access requests should be protected by continuously monitoring their security status (e.g., configuration data, security data, and data related to management functions such as logs) and hardening of its system(s).

8 Reference framework for continuous protection of the service access process

8.1 Overview of the service access process reference framework

It is vital to prevent insecure access to services. While the access environment is continuously changing, traditional mechanisms fall short of meeting the challenges presented by evolving security threats. Instead of traditional perimeter-based security protection and imprecise access control mechanisms, it is crucial to continuously analyse related security status, verify the rationality of access activity, protect the security of the access process and prevent insecure access. This Recommendation defines a reference framework for continuous protection of the service access process.

The reference framework is shown in Figure 1.

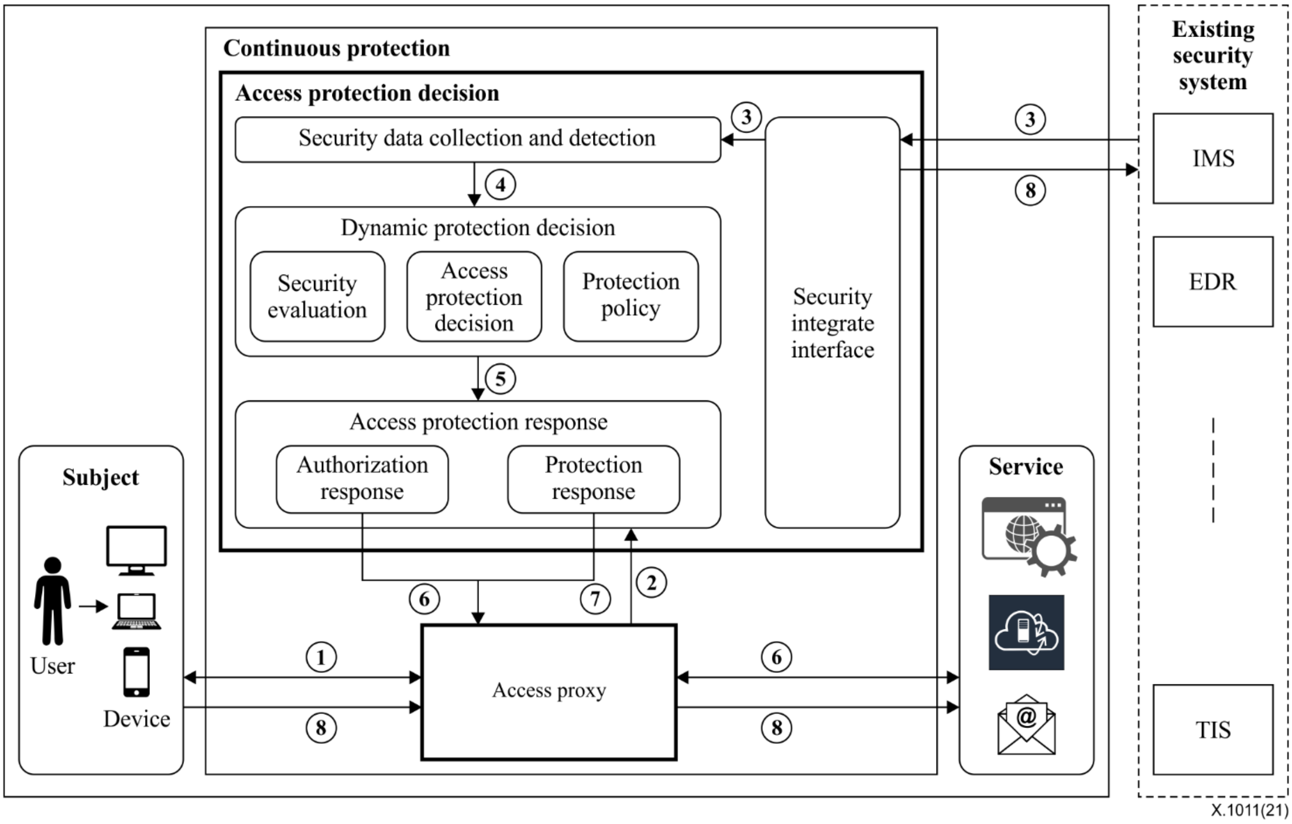

Figure 1 – Reference framework of the service access process

In this framework, *continuous protection* sits between the subject and the service needs to be accessed. The *continuous protection* works after the subject is firstly authenticated. *Continuous protection* consists of two major functional components: *access protection decision* and *access proxy*.

The *access protection decision* continuously collects all the security data relevant to the security of access process, detects security threats, and then makes decision instructions based on both protection policies (e.g., authorization rules such as role based access control (RBAC) rules or attribute based access control (ABAC) rules or protection rules such as making OS run on the latest version) and security status. It may work together with the existing security system, e.g., collects user device detection result from EDR, collects application service detection result from intrusion detection system, etc. Its main function is to give out protection decision instructions.

The *access proxy* enforces the decision instructions made by the *access protection decision*. It should also protect the confidentiality and authenticity of all access traffic.

8.2 Logical functions of continuous protection

Figure 2 shows logical functions of continuous protection.

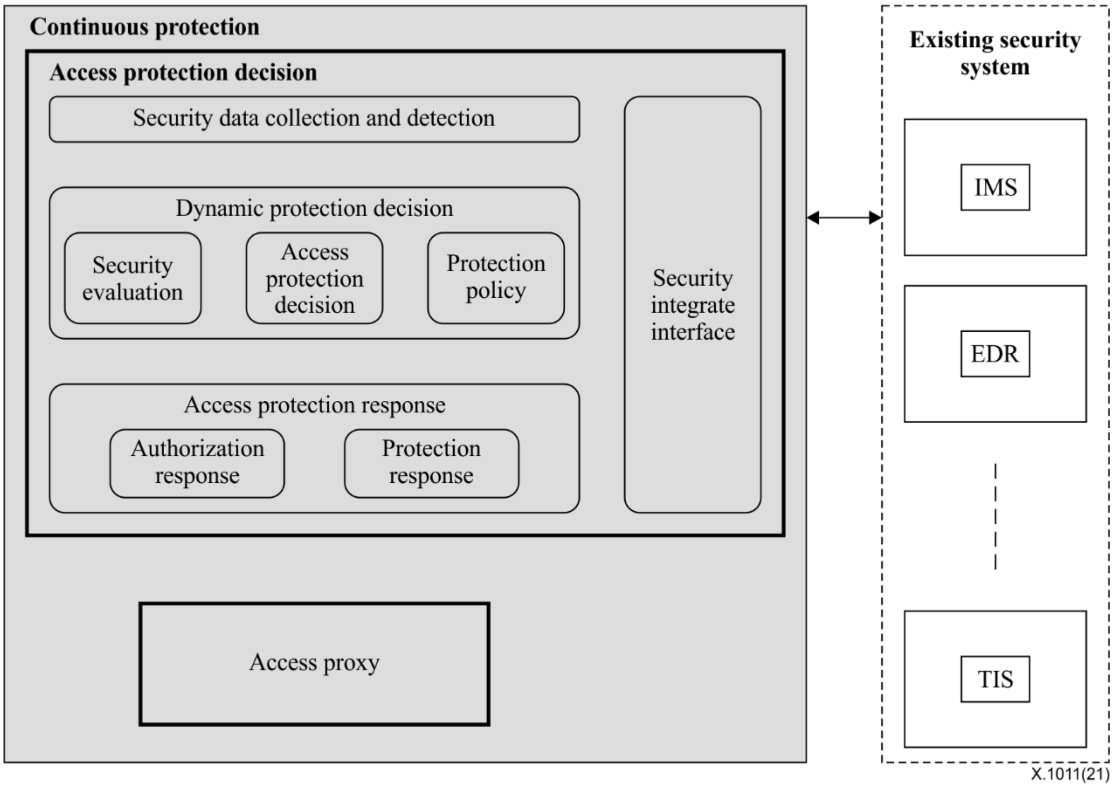
Continuous protection
Access protection decision
Security data collection and detection
Dynamic protection decision
Security evaluation
Access protection decision
Protection policy
Access protection response
Authorization response
Protection response
Security integrate interface
Access proxy
Existing security system
IMS
EDR
TIS
X.1011(21)

Figure 2 – Logical functions of continuous protection

8.2.1 Access protection decision

8.2.1.1 Security data collection and detection (SDCD)

To protect the security of access process, firstly the *access protection decision* needs to collect three types of security data: i.e., raw security data, security result data from the existing security system (e.g., details of the attacker in a security incident, or details of user compliance policy violation, etc.), and threat intelligence data from the existing threat intelligence service (TIS). Raw security data encompass all information relevant to the subject, the service and the communication channels between them, such as:

- user related information, e.g., user account, abnormal behavior, etc.,
- user device related information, e.g., hardware signatures, OS version, vulnerability risk level, etc.,
- application related information, e.g., application signatures, protocols, etc.,
- service-related information, e.g., credential, security log, etc.,
- traffic between the subject and the service.

If possible, it should collect these relevant data from existing security systems through an integrated interface.

By using raw security data and threat intelligence, it should continuously detect activities that could signal a targeted attack aimed at the related entities, e.g., stolen credentials, violation of compliance policy, exploitation of vulnerability, etc.

Then, all security detection results, such as whether the subject is under attack, whether there is a misconfiguration on the user device, etc., and details relevant to detection results will pass to *dynamic protection decision*.

8.2.1.2 Dynamic protection decision

Dynamic protection decision acts as the "brain" of continuous protection and decides how to respond to a subject's access request and security threat. It has three major functional components:

1) *Security evaluation* continuously analyses the security status of all the entities related to access process based on *SDCD*'s detection results. *Security evaluation* results will lead to assign all the entities a "security level". For example, each entity may be tagged with a different indication, such as low-level, medium-level, high-level, etc.

   In order to make an authorization decision instruction, each entity will be assigned with a minimum "security level" required for access by default in *protection policy*. If a subject wants to access a service, the subject's security level must be equal to or greater than the service's minimum "security level" requirement. The authorization decision instruction should also be made on a per-request basis.

2) *Protection policy* includes authorization rules and protection rules. *Protection policy* should update in a timely manner. When the user device and service are first registered (i.e., user's device and service are brought online, connected to the appropriate port and have completed authentication), they should meet the requirements of relevant protection rules, and will be continuously checked during the whole access process, i.e., this process will gather information about the user device and service from *security data collection and detection,* and continuously analyse this information through *SDCD*.

3) *Access protection decision*: There are two types of access protection decision instructions, i.e., authorization decision instructions and protection decision instructions, which will be outlined in the following clauses. The decision instructions are made based on protection policies and the security evaluation results. Authorization decision instructions need to be made in real time so that the *access proxy* can enforce the instructions and all requests can be handled quickly. Protection decision instructions can be made asynchronous, as security evaluation may use technologies such as artificial intelligence and many of the security detection results are relying on external resources. The *access proxy* does not need to wait for them to proceed the access requests. For example, the *dynamic protection decision* can cut down the connection between the subject and the service by making a "cut down connection" protection decision instruction at any time if necessary, the *access proxy* will enforce the instruction and the subject cannot access the service until it receives the "recovery connection" protection decision instruction from the *dynamic protection decision*.

The *dynamic protection decision* should ensure that the subject, the service and all entities between them are in the highest secure status possible during the whole access process.

8.2.1.3 Access protection response

Access protection response has two types:

1) *Authorization response* will receive authorization decision instructions from *Dynamic protection decision*, interpret the instructions (i.e., allowing or denying the access request), and pass the instructions to the access proxy.

2) *Protection response* will receive protection decision instructions from *Dynamic protection decision,* interpret the instructions (e.g., cut down connection, recovery connection, compliance fix instructions, kill insecure processes on the user device, run a script on the service platform, user re-authentication, etc.), pass the instructions to access proxy and the corresponding existing security system via a *security integrate interface*.

8.2.1.4 Security integrate interface

The *security integrate interface* is used for *continuous protection* to interact with existing security systems deployed in an enterprise which are either developed by the enterprise itself or purchased from outside.

The *security integrate interface* has core features as follows:

– Receiving and interpreting results from *security data collection and detection*, then collecting corresponding security data from existing security systems.

– Receiving and interpreting results from *protection response*, directing to existing security systems to be implemented.

– Transforming all data from existing security system into a predefined data format so that external data can be used by *continuous protection*.

8.2.2 Access proxy

8.2.2.1 Features of access proxy

Access proxy is logically served as an authorization policy enforcing point in an enterprise, it verifies the user and user device authentication information and enforces the access protection decision instructions from *dynamic protection decision*. All requests traffic should pass through the *access proxy*.

When the *access proxy* receives an access request from a subject for the first time or when it needs to initiate an additional authentication challenge (e.g., timeout, service modification, etc.), it should authenticate both the user and the user device making the request. This authentication process may be implemented independently either within the *access proxy* or by receiving and verifying authentication information from an existing identity management system (IMS) through a *security integrate interface*.

Access proxy has core features as follows:

– Implements the user and user device authentication function or integrates the authentication function with the existing IMS;

– Acts as a communication channel between the subject and the service, and routes access traffic;

– Implements mutual authentication with both the subject and the service;

– Implements encryption of communication between the subject and the service;

– Enforces the authorization decision instructions (i.e., granting or denying access requests) made by *dynamic protection decision*;

– Enforces the protection decision instructions (i.e., cutting down the connection between the subject and the service) made by *dynamic protection decision*;

– Implements load balance for the services; and,

– Logs all access requests.

8.2.2.2 Model of access proxy

In order to ensure that every single access request from the subject is properly authorized, a logical access gateway is an implementation model of *access proxy*. It centralizes requests logging for performing secure analysis more quickly. The model of access proxy is shown as Figure 3.

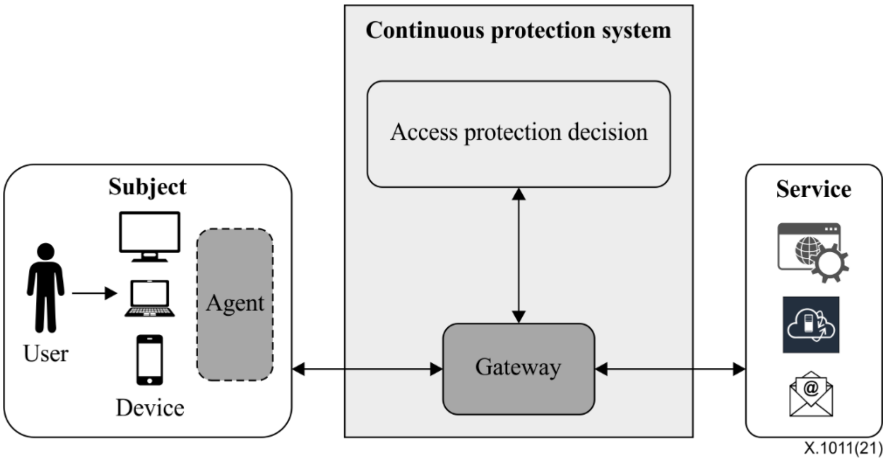

Figure 3 – Model of access proxy

In this model, the *access proxy* is composed of an agent and a gateway. All access requests from subjects will be routed to the logical gateway through the agent, then the gateway passes them to the service. That means, the subject with access request will not directly connect to the service. This will ensure that all request flows are authenticated, authorized and transmitted via a secure communication channel.

From deployment point of view, the agent may be implemented in different ways depending on service types and whether the enterprise has enough control (such as to install software on the user device, integrate an software development kit (SDK) within an application on the user device, configure a web proxy for the browsers, etc.) of the user device making the access requests. The gateway may adopt a centralized deployment in front of the service server or as a gateway software installed on the service server.

In the case of the subject and the service that may have already implemented a secure communication channel, the gateway may not be needed.

8.3 Workflow

The workflow of the continuous protection mainly consists of the following steps:

Step 1. A subject requests a service via an *access proxy*. Then the subject and the *access proxy* verify each other with the user's identity, the user device's identity and the identity of *access proxy*.

Step 2. When mutual authentication succeeds, the *access proxy* requests authorization from the *access protection decision*.

Step 3. The *security integrate interface* collects relevant data (i.e., raw security data, security result data, threat intelligence data) from existing security systems.

Step 4. The *security data collection and detection* sends the security evaluation results and related detailed information to the *dynamic protection decision*, then the access protection decision instructions on authorization and protection are made according to the security policies.

Step 5. The access protection decision instructions on authorization and protection are sent to the *access protection response*. Then, the *authorization response* and the *protection response* execute the authorization decision instructions and the protection decision instructions respectively and send proper results out.

Step 6. The authorization result is transferred from the *authorization response* to the *access proxy*, the *access proxy* processes the result as below:

- If the result is to permit the access, then the *access proxy* forwards the access request to the target server, and then returns the responses from the target server to the subject.
- If the result is to block the access, then the *access proxy* refuses the subject's request directly.

Step 7. Once an access is permitted successfully, the *dynamic protection decision* makes protection decision instructions continuously according to the subsequent actions and status in the entire access process. The *access protection response* keeps receiving these instructions, executing them and sending results to the *access proxy* and the *security integrate interface* which process these results accordingly.

Step 8. According to the protection decision instructions, possible actions from the *access proxy* include cutting down connection, restoring connection, etc. As the *security integrate interface* works together with the existing security system, the *protection response* can be system hardened, killing insecure processes on the user device, as well as user re-authentication, etc.

Appendix I

Typical application scenarios

(This appendix does not form an integral part of this Recommendation.)

Scenario 1: Teleworking

Figure I.1 shows a teleworking scenario.

1) **Scenario description**

In this scenario employees of an enterprise need to access a routine system called Customer Relationship Management, an IT service which is deployed in an Intranet via Internet from home, to submit business requests or approve documents. Engineers in the enterprise need to login to servers to do daily updates for their website services, or carry out troubleshooting tasks in urgent cases (for example, if they cannot come to the office due to adverse weather conditions).

2) **Current problems**

The traditional way of teleworking is to use a virtual private network (VPN) to connect from home to Intranet services. This system has the following disadvantages:

a) When connecting to services, the VPN system does not check the security of the devices, so it cannot prevent attackers using compromised legal devices as a stepping stones to attack the enterprise's Intranet.

b) After being authenticated by VPN, the subject can connect to the Intranet by default, and it cannot provide fine-grained access control.

c) Due to deployment with hardware and dependency on the VPN vendor, it is not easy to implement a rapid system expansion when access demands increase suddenly.

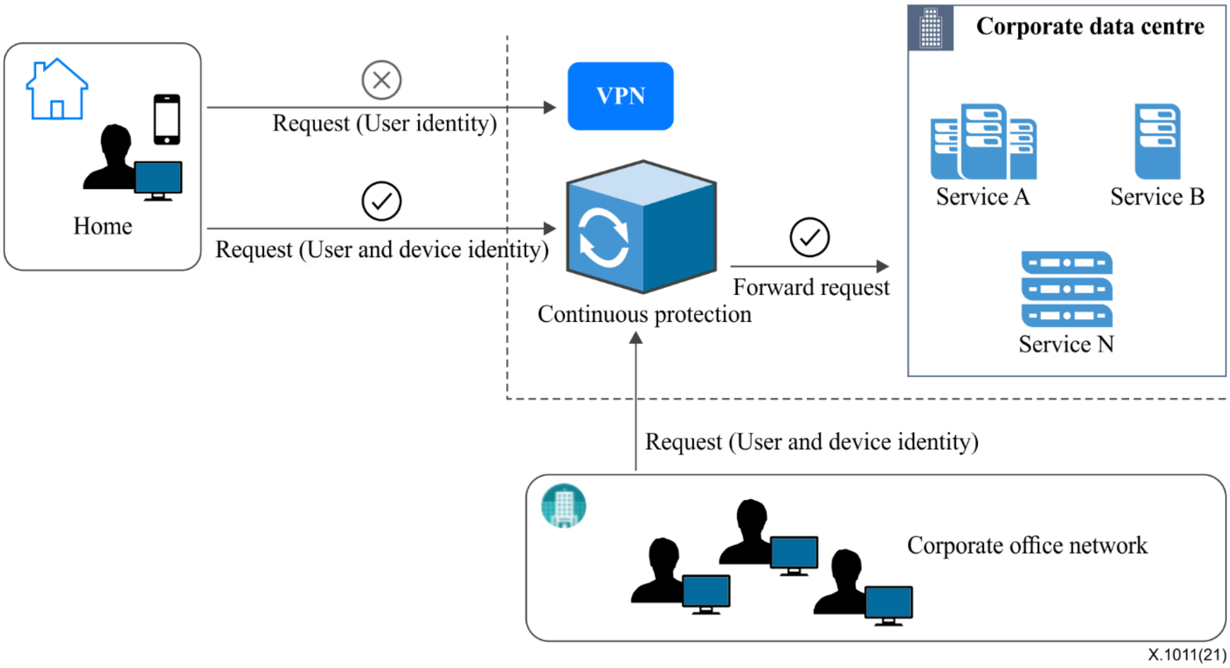

Figure I.1 – Teleworking scenario

3) **Benefits of deployment of continuous protection**

a) Stronger awareness of a device's security status helps in making more precise authorization decision, in the case of attackers who may impersonate normal users by having gained access to devices.

b) The attack surface of services is shrinking, because all services are deployed behind continuous protection, only the continuous protection is visible over the Internet and to attackers.

c) Whether in the office or from home, it is almost the same access process, so employees will get better user experience and even stronger security.

d) It is easier to expand continuous protection via software implementation and load balancing methodologies.

Scenario 2: Access to multi-cloud services

Figure I.2 shows a multi-cloud accessing scenario.

1) **Scenario description**

Small and medium-sized enterprises often purchase multiple public clouds to deploy their applications for better stability. Different vendors provide different ways of accessing their cloud services.

2) **Current problems**

It is hard for small and medium-sized enterprises to keep track of different vender's access methods, and is also difficult to maintain a single access control policy to fulfil the enterprise's security demands.

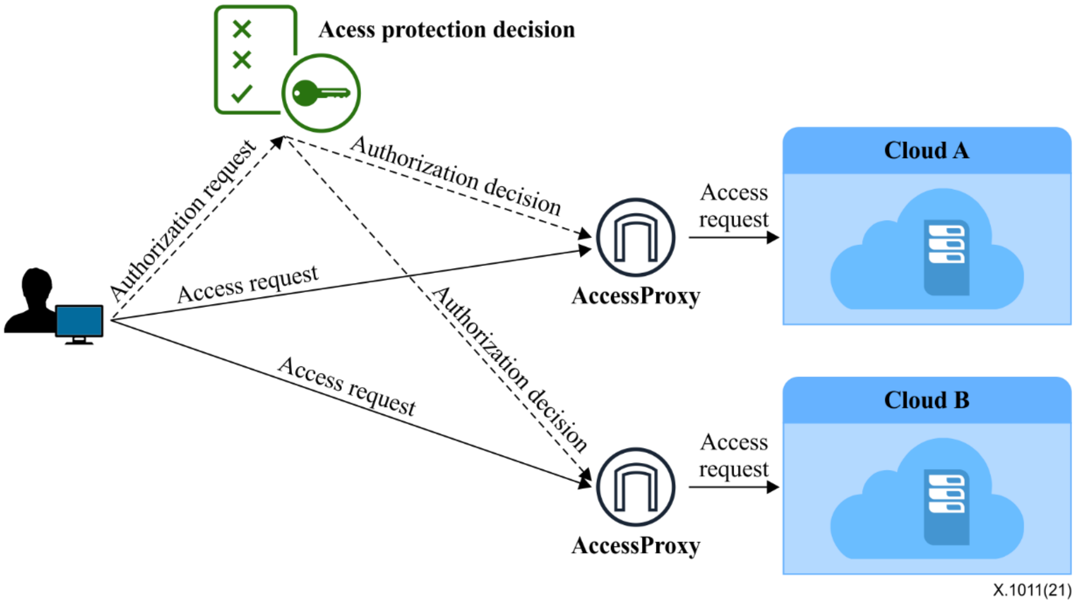

Figure I.2 – Multi-cloud accessing scenario

3) **Benefits of deployment of continuous protection**

a) The same access protection decision component could potentially be used to manage the access to multi-cloud services. Users do not need to maintain multiple access interfaces, and can use one access control policy to manage different cloud's resources.

b) Each cloud service is hidden behind its access proxy, so that the virtual server port is invisible to attackers.

c) Distributed deployment of access proxy will help avoid attacks such as distributed denial of service (DDoS) attacks.

Scenario 3: Server to server communication

Figure I.3 shows a server to server communication scenario.

1) **Scenario description**

Traffic between server to server is increasing heavily because of increasing numbers of cloud-native micro-service based applications and enterprises' applications that are becoming more complicated. Many services components need communicate with each other so that access requests are coming from servers rather than individuals.

2) **Current problems**

In the perimeter-based concept, the identity and authority of inside servers are rarely checked. But to prevent inside threats such as launching of lateral movement attacks through a compromised server it is necessary to make sure that every access request is carefully checked.

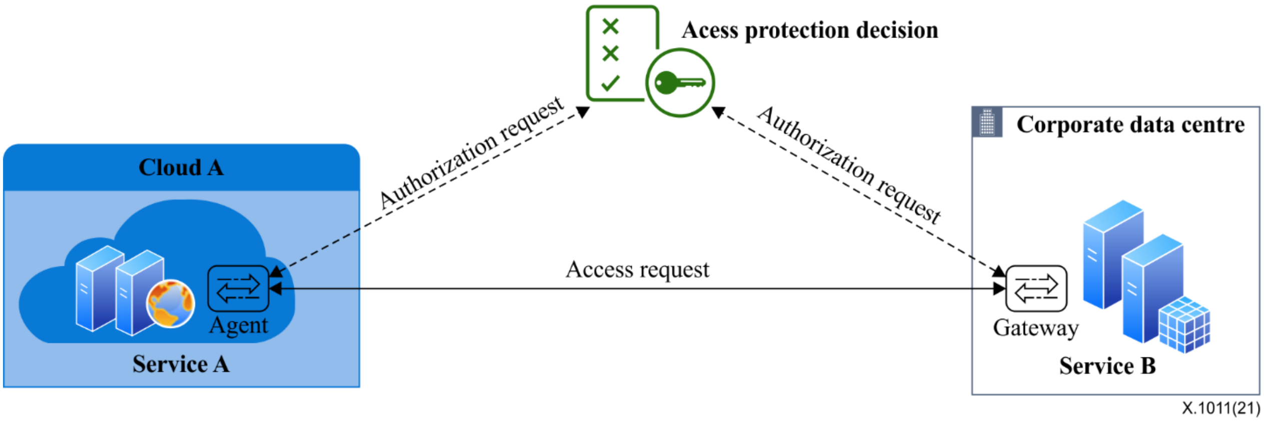

Figure I.3 – Server to server communication scenario

3) **Benefits of deployment of continuous protection**

a) It can be used for any server-to-server communication scenario.

b) It helps to protect every service regardless of whether the server is in the enterprise's Intranet data centre or under another outside provider's infrastructure.

Bibliography

[b-ITU-T X.800]	Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
[b-ITU-T X.1252]	Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.
[b-ITU-T Y.2720]	Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021