国际电信联盟
电信标准化部门

建议书

ITU-T X.1644 (03/2023)

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全最佳做法和导则

分布式云的安全指南

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	**X.1640–X.1659**
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1644建议书

分布式云的安全指南

摘要

ITU-T X.1644建议书分析了分布式云的安全威胁和挑战，提出了针对分布式云威胁的安全指南，其中包括核心云、区域云和边缘云的安全指南。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1644	2023-03-03	17	11.1002/1000/15112

关键词

云计算、分布式云、安全指南

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1644建议书

分布式云的安全指南

1 范围

本建议书分析了分布式云的安全威胁，提供了分布式云的安全指南。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1408] ITU-T X.1408建议书（2021年），基于分布式账本技术的数据访问和共享的安全威胁和要求。

[ITU-T X.1601] ITU-T X.1601建议书（2015年），云计算安全框架。

[ITU-T Y.3500] ITU-T Y.3500建议书（2014年），信息技术 – 云计算 – 概述与词汇。

[ITU-T Y.3508] ITU-T Y.3508建议书（2019年），云计算 – 分布式云概述和高级要求。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 云功能类型（cloud capabilities type）[ITU-T Y.3500]：建立在使用资源的基础上，云服务向云服务客户提供的功能类别。

注 – 云功能类型为应用功能类型、基础设施功能类型以及平台功能类型。

3.1.2 云计算（cloud computing）[ITU-T Y.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.3 云服务（cloud service）[ITU-T Y.3500]：通过使用定义的接口启动的、由云计算实现的一种或多种功能。

3.1.4 云服务客户（cloud service customer）[ITU-T Y.3500]：为使用云服务而具有业务关系的一方。

注 – 业务关系不一定意味着财务协议。

3.1.5 云服务提供商（cloud service provider）[ITU-T Y.3500]：提供云服务的一方。

3.1.6 边缘云（edge cloud）[ITU-T Y.3508]：部署在云服务客户（CSC）访问的网络边缘的云计算、利用小容量资源实现云服务。

注1 – 边缘云上启用的云服务是由云服务提供商（CSP）根据云服务类别提供的轻量级云服务。

注2 – 轻量级云服务是指云服务的一部分，将云服务功能重新配置，以适应边缘云，如小容量资源的基站和网关。

3.1.7 威胁（threat）[ITU-T X.1408]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 核心云：一组集中的服务，包括云计算网络中的所有不受地域限制的服务、对时延不敏感的服务、计算高度密集型服务、备份和恢复服务以及高安全级别服务。

3.2.2 分布式云：分布式云是经典云计算概念的延伸，将云计算功能进一步扩展到网络边缘。

3.2.3 区域云：一种可选择性部署的核心云，用于在核心云和边缘云之间进行高效配置，以减少核心云的负载。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

API 应用服务接口

CC 核心云

CSC 云服务客户

CSP 云服务提供商

DDoS 分布式拒绝服务

DoS 拒绝服务

EC 边缘云

IoT 物联网

OTA 无线

REST 表述性状态转移

TLS 传输层安全

VPN 虚拟专用网络

XML 可扩展标记语言

XSS 跨站脚本攻击

5 惯例

本建议书中：

关键词“**要求**”（**is required**）表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“**建议**”（**is recommended**）表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

6 概述

分布式云方兴未艾，因为越来越多的时延敏感性服务（如视频和物联网（IoT）服务）需要更快的响应速度；它是传统云计算的延伸，并将其功能进一步扩展至网络边缘。它可以提供的本地化云服务更接近客户和数据源，而且可以与其它云交互，提供分布式、低时延、高性能的服务。

分布式云包括将云功能类型分布到网络边缘，通过物理或虚拟资源池之间的互通，在有限的带宽上实现低时延和实时处理的云服务[ITU-T Y.3508]。典型的分布式云如图6-1所示，包括核心云、区域云和边缘云。

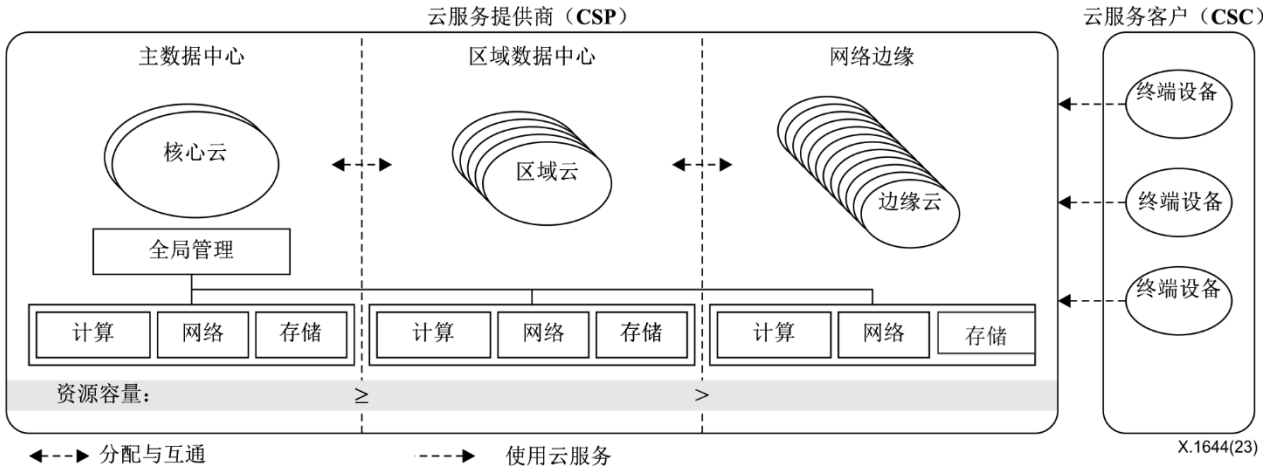

图6-1 – 分布式云的概念

核心云拥有较大的资源容量和全局管理点，可以控制分布式云中的云资源。核心云支持计算强度高、不受地域限制的云服务。

区域云可选择性地部署在来自核心云的特定区域，以实现负载分担和服务质量增强。区域云处理来自由核心云全局管理控制区域的云服务请求。

注1 – 区域云通过为某一特定区域的云服务客户（CSC）执行定制化云服务，实现比核心云更短的时延。假设从CSC到区域云的网络时延低于从CSC到核心云的网络时延，且核心云和区域云之间的云服务执行时间差异可以忽略不计。

注2 – 区域云对云服务负载和来自核心云的数据缓存进行缓冲，并将它们提供给区域内的CSC。

边缘云部署在CSC访问的网络边缘，资源容量较小。边缘云专门需要专用的硬件资源；例如边缘云中的资源由于空间或功率局限而受到限制。根据CSC的云服务需求和部署环境的条件，边缘云可能具有不同的资源配置和云功能类型，包括物理资源和虚拟资源。

7 分布式云的安全挑战和威胁

使用分布式云具有高速度、高效率和高性能方面的优势。分布式云中的核心云、区域云和边缘云会带来新的安全挑战和威胁[ITU-T X.1601]。

7.1 核心云的安全挑战和威胁

分布式云具有不同规模的基础设施，核心云或区域云的资源容量大，边缘云的资源容量小。核心云利用异构的基础设施作为单一系统，为分布式云中的CSC提供各种服务。核心云的安全挑战和威胁如下：

a) **系统漏洞**：分布式云基础设施包含系统漏洞，尤其是在拥有复杂基础设施和多个第三方平台的网络中，核心云的漏洞也会影响到区域云和边缘云。

b) **物理损坏**：分布式云基础设施可能被部署在不可信的物理环境中，可能会受到恶意用户、恶劣天气或地震等造成的物理损坏。核心云的物理损坏也可能影响区域云和边缘云的安全。

7.2 区域云的安全挑战和威胁

a) **传输拦截**：核心云需要与区域云进行数据传输，这些传输链路可能遭遇拦截。

b) **假冒的命令或请求**：来自假冒的核心云、区域云或边缘云的恶意命令或请求可能导致数据泄漏。

c) **接口攻击**：由于核心云通过开放接口与多个区域云连接，因此可能会通过这些接口遭受攻击。

d) **天坑（sinkhole）攻击**：入侵者能够损害设备或在网络内部引入假冒设备，并使用该设备发起天坑攻击。天坑攻击是一种网络层的攻击，当中，遭受攻击的设备向其邻近设备发送虚假路由信息，将网络流量吸引至其自身。

e) **流氓网关**：部署流氓网关对攻击者而言很容易。一旦合法设备被诱骗连接到流氓网关，就可以收集机密的连接信息。这将有效地规避许多现有的安全措施，并可能对官方组织装置造成无线电干扰。

f) **未经授权访问物联网网关**：攻击者可能使用未经授权的方式访问物联网网关，这可能导致敏感信息泄露、数据修改和非法使用边缘云的一些资源。

7.3 边缘云的安全挑战和威胁

a) **多租户问题**：许多云解决方案未在客户端之间提供必要的安全保护，导致资源、应用和系统的共享。在这种情况下，威胁可能来自云计算服务中的其他客户端，针对一个客户端的威胁也可能对其他客户端产生影响。

b) **假冒请求**：如果请求从假冒的区域云或边缘云发出，而核心云未能识别，可能导致数据泄漏等。

c) **跨站脚本（XSS）攻击**：跨站脚本攻击可以利用网站中存在的漏洞，在客户机中注入恶意代码，冒用用户凭证，从事恶意活动。

d) **可扩展标记语言（XML）包装**：XML是底层的标记语言，能够对边缘云中的应用程序进行来源认证。黑客可以利用XML重写或签名包装技术发起账户劫持攻击。

e) **员工疏忽**：员工疏忽仍然是所有系统最大的安全问题之一，但对分布式云管理的威胁尤其严重。员工可能从他们的手机、家用平板电脑和家用个人电脑登录分布式云管理平台，有可能导致系统面临许多外部威胁。

f) **网络钓鱼和社会工程攻击**：由于分布式云系统的开放性，网络钓鱼和社会工程攻击已经变得特别普遍。一旦获取了登录信息或其他机密信息，恶意用户就有可能轻而易举地侵入系统。

g) **丧失控制权**：当一个组织的服务被放在分布式云上时，他们就丧失了控制权，不知道这些服务在云中可存储位置。同时，从用户的角度来看，这变成了一个严重的安全问题，因为用户不知道有什么安全机制来保护他们的服务。

h) **假冒设备**：攻击者可能会伪装成合法设备，并向边缘云发送虚假或恶意数据，或窃取用户的数据。

i) **边缘设备捕获**：边缘云附近有许多终端设备，可以收集数据，将数据传输到边缘云，并从边缘云接收结果或命令。由于终端设备的安全保护薄弱，很容易被攻破。

j) **分布式拒绝服务（DDoS）攻击**：针对分布式云的DDoS攻击的可行性大大增加。如果向云计算系统发起足够的恶意流量，计算系统就会完全崩溃或遇到困难。特别是，边缘云是相对较小的云实体，安全保护相对薄弱，因此更容易被黑客攻击并用于DDoS攻击或其他非法活动。

k) **虚拟化安全**：在边缘云环境下，虚拟化安全包括对基于虚拟化技术的边缘网关、控制器和服务器实施安全隔离和增强。与核心云和区域云相比，这些存储和计算资源有限的边缘节点面临着更加复杂和广泛的攻击向量。

8 分布式云的安全指南

本条款给出了与第6条所述的分布式云系统的核心云、区域云和边缘云相关的安全指南。

8.1 核心云的安全指南

核心云的安全指南包括核心云系统的安全指南、物理安全指南、拒绝服务安全指南和边缘设备的安全指南。

8.1.1 核心云系统安全

核心云系统的安全指南如下：

a) 建议采用漏洞事件响应工具。

b) 建议使用文件扫描、应用程序白名单、基于机器学习的恶意软件检测和网络流量分析等技术来防止恶意软件进入云服务。

c) 建议审查和更新风险评估以包括云服务。识别并解决核心云环境和提供商引入的风险因素。利用云提供商的风险数据库加快评估过程。

8.1.2 物理安全

物理安全指南如下：

a) 建议在适当的位置建设核心云基础设施，避免机场起降通道、发电厂、洪泛区、地震断层线或其它自然灾害多发地区。

b) 建议为地下基础设施物理环境条件的变更、维护和监测提供流程。

c) 建议为地下基础设施提供冷却系统和合规标准。

d) 建议限制来自核心云基础设施的入口点，以降低物理入侵的风险。

e) 建议在整个核心云基础设施中提供多个检查点，以最大程度地降低恶意入侵者获得访问权限的风险。

f) 建议使用监控系统提供额外的物理安全。

g) 建议使用冗余来帮助核心云基础设施以最少的停机时间应对任何事件。

8.1.3 抗拒绝服务攻击

拒绝服务指南如下：

a) 建议核心云服务器容量足够处理大量流量峰值，并拥有解决安全问题所需的缓解工具。

b) 建议定期更新和修补防火墙和网络安全程序。

8.2 区域云的安全指南

区域云的安全指南包括传输数据和静态数据、开放接口以及物联网网关的安全指南。

8.2.1 传输数据和静态数据安全

区域云为某个地理区域提供部分或完整的核心云服务。区域云中的传输数据和静态数据的安全指南包括以下方面：

a) 要求区域云使用一定强度的加密对通信和数据进行加密。亦建议支持安全传输协议服务，以避免基于协议的攻击破坏机密性。

b) 要求区域云对服务身份进行认证和识别，并采取严格的安全隔离和访问控制策略。要求支持访问控制策略的定制和管理。

c) 建议区域云支持安全的数据交换系统，实现对数据格式、内容、流量等的实时监控。

d) 建议安全数据交换系统满足云环境下的各种弹性需求，包括提供灵活的部署方式、灵活的资源调度方式、基于业务强安全隔离的安全数据交换方法等。

e) 建议区域云支持传输数据的恶意代码检测和清除。

f) 要求采用加密和验证机制保证本地存储的完整性和机密性，包括系统管理数据（如索引文件、云服务信息和密钥）、认证信息和重要业务数据（如用户隐私数据）。

g) 建议数据访问支持基于角色的身份认证，对非法访问采取严格的访问控制措施。

8.2.2 开放接口安全

云服务提供商（CSP）需要提供网络接口和应用程序编程接口（API），以便能够配置、管理、协调和监测各种云服务，以及直接提供服务。第三方通常会在这些接口的基础上进行开发以提供额外的服务。区域云的安全API指南如下：

a) 要求对表述性状态转移（REST）API使用加密，如传输层安全（TLS）或其他加密方法，在传输过程中加密数据并防止篡改。亦要求使用签名机制，以确保只有具有访问权限的用户才能解密和修改数据。

b) 建议通过令牌建立API的可信身份，然后只有拥有令牌的可信身份才能访问和控制服务和数据资源等。

c) 建议对开放API接口的调用行为和异常数据传输进行实时监控并发出警告，如限制API接口的访问频率。

d) 建议主动识别API的漏洞。检测工具可用于检测API安全和数据泄露，并实时跟踪API是否受到攻击以及是否有漏洞被利用。

e) 建议使用API安全网关，因为这项技术已被用作保护API安全的关键技术。由于API安全网关可用于控制和管理API接口的使用，它还可以对使用API接口和服务的用户进行身份验证。

8.2.3 物联网网关的安全

物联网设备通过物联网网关连接到互联网，成为恶意软件和网络攻击的主要目标。物联网网关的安全指南如下：

a) 建议物联网网关支持设备认证和访问控制；只允许授权用户和设备访问，并实施安全存储或保险库（vault），以保护密钥和证书等机密信息。

b) 建议物联网网关支持策略管理，配置访问权限，根据安全策略控制设备对应用服务（技术服务、业务服务、数据服务）、文件（配置文件、日志文件、镜像文件）和其他对象的访问，网关能够及时中断非法连接和会话。

c) 建议物联网网关启用无线（OTA）更新，确保网关运行最新的软件和固件，避免常见的漏洞和风险。安全启动可以确保网关以其完整性和真实性已被加密和验证的固件镜像启动，防止使用恶意的固件启动网关。

d) 建议物联网网关支持各种安全控制措施，以保护物联网设备。例如，当物联网网关被用作网络和设备的安全代理时，建议在网关中执行防火墙、基于规则的流量过滤和白名单功能。

e) 建议物联网网关支持细粒度的事件日志，以便更深入地了解网关中运行的进程，进行安全审计。

8.3 边缘云的安全指南

边缘云安全指南包括边缘云基础设施的安全指南、传输数据和静态数据边缘云网络的安全指南、万维网安全指南和边缘云上终端设备的安全指南。

8.3.1 边缘云基础设施安全

边缘云基础设施提供硬件和软件基础，边缘基础设施安全是边缘云的基本要求。边缘云基础设施的安全指南如下：

a) 建议提供不依赖于硬件的轻量级虚拟化框架，并实施安全隔离和增强机制。

b) 建议加强超级管理程序（hypervisor）自身的安全防护，减少攻击向量。

c) 建议与边缘云服务器合作，提供操作系统（OS）恶意代码检测与预防、应用程序强安全隔离、支持可信执行环境等关键机制，保证OS上运行的各种应用程序的机密性和完整性，因为它们的计算或存储资源有限，安全策略和机制可能无法与核心云或区域云及时同步。

d) 建议边缘云提供商以自动、透明和轻量级的方式实施识别和认证过程。因为分布式云的边缘节点和动态网络结构可能会导致重复识别和认证。

8.3.2 边缘云网络安全

由于边缘节点数量众多，网络拓扑复杂，增加了攻击路径，攻击者很容易向边缘云节点发送恶意网络数据包或发起拒绝服务攻击，影响边缘云网络的可靠性。边缘云网络的安全指南如下：

a) 建议在设计和实施阶段确保协议安全，边缘云利用其满足CSC的不同数据传输需求。

b) 建议为潜在易受攻击的协议添加额外的安全策略，例如通过在网关中添加模块，实现数据通过虚拟专用网络（VPN）、TLS或其他安全通道传输。

c) 建议对属于不同域的虚拟机之间的网络传输进行完整性和安全性验证，以确保不同业务通信单元之间的有效隔离。此外，隔离模块可以由可视化环境中的控制器调度，以提供隔离功能。

d) 建议对网络流量进行安全监控，及时报警安全事件，高效进行事件响应。此外，保护系统可以直接阻止恶意流量。

8.3.3 边缘云万维网安全

万维网安全指南如下：

a) 建议确保对边缘云系统设施进行有效的远程监控。

b) 建议边缘云安全伴随着广泛的教育工作。告知员工能够/不能使用什么设备，并帮助他们识别安全风险。

c) 建议确保老旧过时设备不与更复杂的设备放在一起，以减少网络中的漏洞点。

8.3.4 边缘云中终端设备的安全

边缘云中终端设备的安全指南如下：

a) 建议在未经授权的个人设备试图接入边缘云数据时阻止接入。

b) 建议配置边缘的功能时包括强认证和加密认证节点等特性。

c) 建议IT安全协议管理哪些设备可以接入边缘云系统网络以及接入条件。

d) 建议实施并持续监测边缘云环境。

e) 建议假设边缘设备已遭到破坏，而不是自动相信来自设备的信息，所有数据都可能是恶意的，除非证明其并非恶意。

f) 建议只有经过认证的边缘设备才能接入核心云并向其传输数据。

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦