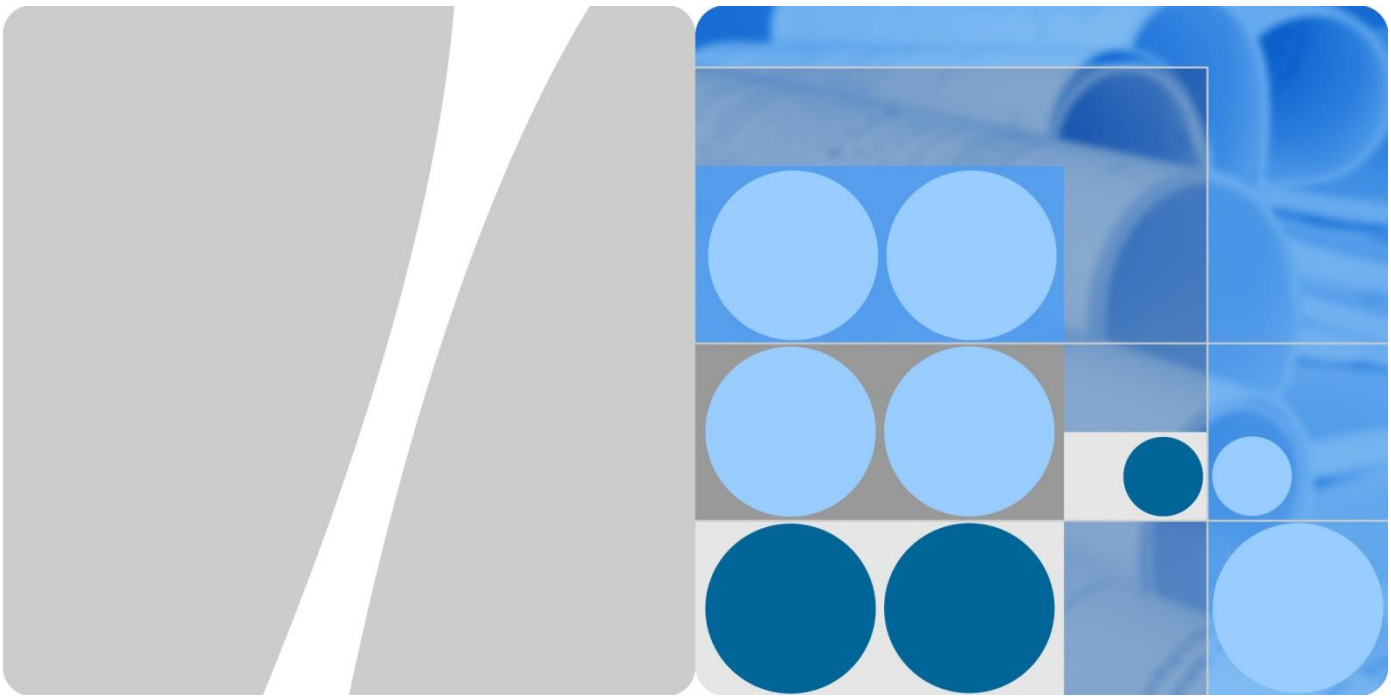
资料编码



华为 USG9500 系列下一代防火墙安全技术白皮书

文档版本 V1.3

发布日期 2017-08-08

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目　录

1 简介

1.1 USG9500 产品概述

USG9500系列产品是华为技术有限公司（以下简称华为）面向大中型企业、小型企业或分支机构以及电信运营网推出的新一代电信级统一安全网关设备。USG9500系列产品可广泛应用于运营商、企业、政府、金融、能源、学校等网络边界。 可以同时满足百兆、千兆、万兆统一安全网关的市场需求。USG9500系列产品拥有丰富的接口扩展能力，支持多种接口卡其中包括万兆以太网接口卡。USG9500系列产品在基本防火墙功能基础上还支持丰富的UTM（Unified Threat Management）功能，致力于内容安全防护、上网行为管理等方面，为用户提供全方位的安全防护。如图所示，USG9500系列产品放置于网络出口处，有效阻止Internet 上的黑客入侵、DDoS 攻击，阻止内网用户访问非法网站，限制带宽，为内部网络提供一个安全可靠的网络环境。

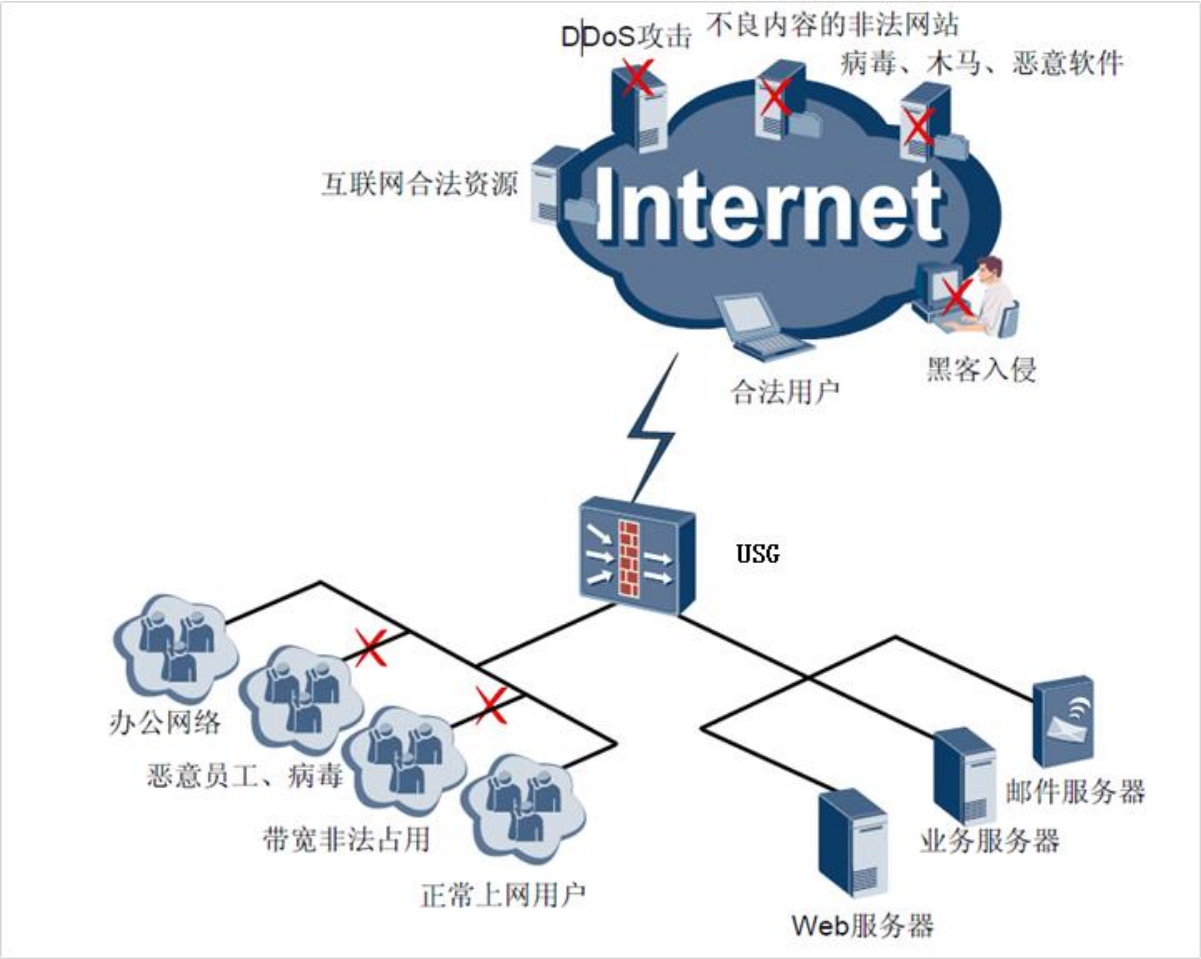


图 1 USG9500 产品典型应用场景

1.2 USG9500 产品所面临的安全威胁

管理层安全威胁

缺乏安全管理规章制度，或者没有严格执行安全管理规章制度。

人员安全意识不足。

没有及时进行系统及应用安全补丁的安装，导致系统存在安全漏洞。

多人共用帐号，责任无法追溯。

安全资料不全，无法有效指导安全生产。

应用层安全威胁

输入验证：缓冲区溢出，跨站点脚本编写，SQL 注入。

身份验证：网络窃听，暴力破解，词典攻击，重放 cookie，盗窃凭据。

授权：提高特权，泄漏机密数据，篡改数据，引诱攻击。

配置管理：未经授权访问管理接口，未经授权访问配置存储器，检索明文配置数据，缺乏个人可记帐性，越权进程和服务帐户。

敏感数据：访问存储器中的敏感数据；窃听网络；篡改数据。

会话管理：会话劫持；会话重放；中间人。

加密技术：密钥生成或密钥管理差；脆弱的或者自定义的加密术。

参数操作：查询字符串操作；窗体字段操作；cookie 操作；HTTP 标头操作。

异常处理：信息泄漏；拒绝服务。

安全审计：用户拒绝执行某项操作；攻击者利用没有跟踪记录的应用程序；攻击者掩饰他或者她的跟踪记录。

系统层安全威胁

病毒、特洛伊木马和蠕虫：病毒就是一种设计的程序，它进行恶意的行为，并破坏操作系统或者应用程序。除了将恶意的代码包含在表面上是无害的数据文件或者可执行程序中外，特洛伊木马很像一种病毒。除了可以从一个服务器自我复制到另一个服务器，蠕虫类似于特洛伊木马。蠕虫很难检测到，因为它们不是定期创建可以看见的文件。通常只有当它们开始消耗系统资源时，才能注意到它们，因为这时系统运行缓慢或者其他执行的程序停止运行。

足迹：足迹的示例有端口扫描、ping 扫描以及 NetBIOS 枚举，它可以被攻击者用来收集系统级的有价值信息，有助于准备更严重的攻击。足迹揭示的潜在信息类型包括帐户详细信息、操作系统和其他软件的版本、服务器的名称和数据库架构的详细信息。

破解口令：如果攻击者不能够与服务器建立匿名连接，他或者她将尝试建立验证连接。为此，攻击者必须知道一个有效的用户名和口令组合。如果您使用默认的帐户名称，您就给攻击者提供了一个顺利的开端。然后，攻击者只需要破解帐户的口令即可。使用空白或者脆弱的口令可以使攻击者的工作更为轻松。

拒绝服务：可以通过多种方法实现拒绝服务，针对的是基础结构中的几个目标。在主机上，攻击者可以通过强力攻击应用程序而破坏服务，或者攻击者可以知道应用程序在其上寄宿的服务中或者运行服务器的操作系统中存在的缺陷。

任意执行代码：如果攻击者可以在您的服务器上执行恶意的代码，攻击者要么就会损害服务器资源，要么就会更进一步攻击下游系统。如果攻击者的代码所运行的服务器进程被越权执行，任

意执行代码所造成的危险将会增加。常见的缺陷：允许遍历路径和缓冲区溢出攻击的未打补丁的服务器，这种情况可能导致任意执行代码。

未授权访问：不足的访问控制可能允许未授权的用户访问受限制信息或者执行受限制操作。

网络层安全威胁

信息收集：可以用与其他类型系统相同的方法发现网络设备并对其进行剖析。通常，攻击者最初是扫描端口。识别出开放端口后，他们利用标题抓取与枚举的方法检测设备类型，并确定操作系统和应用程序的版本。具有这些信息后，攻击者可以攻击已知的缺陷，这些缺陷可能没有更新安全补丁。

嗅探：嗅探查或者窃听 就是监视网络上数据（例如明文密码或者配置信息）传输信息的行为。利用简单的数据包探测器，攻击者可以很轻松地读取所有的明文传输信息。同时，攻击者可以破解用轻量级散列算法加密的数据包，并解密您认为是安全的有用负荷。探查数据包需要在服务器/客户端通信的通道中安装数据包探测器。

欺骗：欺骗就是一种隐藏某人在网上真实身份的方式。为创建一个欺骗身份，攻击者要使用一个伪造的源地址，该地址不代表数据包的真实地址。可以使用欺骗来隐藏最初的攻击源，或者绕开存在的网络访问控制列表（ACL，它根据源地址规则限制主机访问）。

会话劫持：也称为中间人攻击，会话劫持欺骗服务器或者客户端接受：上游主机就是真正的合法主机。相反，上游主机是攻击者的主机，它操纵网络，这样攻击者的主机看上去就是期望的目的地。

拒绝服务（DoS/DDoS）：拒绝服务就是拒绝合法用户访问服务器或者服务。

2 USG9500 产品安全解决方案

2.1 安全架构

参考通信系统安全模型 (ITU-T X.800)，安全架构由三个安全层次 (Layer)，三个安全平面 (Plane)，八个纬度组成，并且基于每个层次和每个平面可能存在的威胁，提供了对应的安全技术方案，详细架构如下图所示：

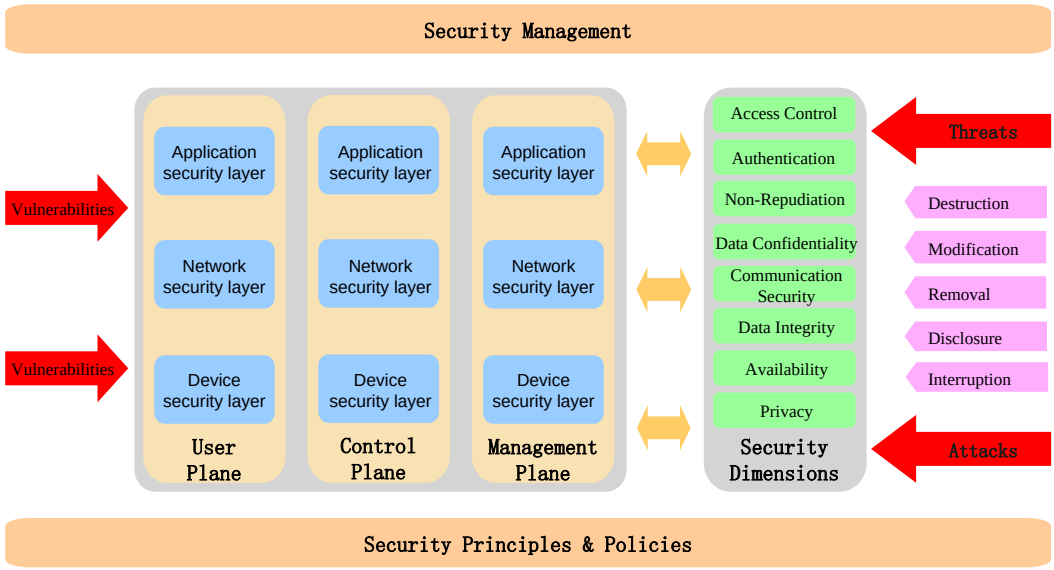


图 2 安全架构

三个安全层、三个安全平面和八种安全纬度并不是平行的，而是相互交叉在一起的，下面先对这些安全纬度进行介绍。

2.2 安全维度

根据ITU-T X.800协议的描述，电信系统的安全风险和攻击主要有如下种类：

Destruction：破坏，对信息或其它资源的破坏。

Modification：篡改，对信息的篡改。

Removal：删除，信息或其它资源地窃取、删除或丢失。

Disclosure：信息泄露。

Interruption：服务中止。

USG9500 设备通过以下 8 个安全纬度对这些攻击和威胁进行安全防护。

2.2.1 访问控制/Access Control

常用于防止对网络资源进行未授权的访问和调用。例如从非受信网络到受信网络的访问，通过接入控制策略保护被访问系统不受恶意行为的影响。访问控制是一种常见的网络控制技术。

USG9500产品提供丰富的访问控制技术，如单用户的ACL访问控制列表，全局的基于MAC的，基于源目地址，基于应用的ACL等。

2.2.2 认证/Authentication

认证，在进入网络或系统前，需要有安全机制确保其是否具有合法身份。例如对操作者登录帐号进行校验。

USG9500产品的所有用户及系统组件间的访问都需要经过鉴权才可以访问，为了防止未授权用户通过暴力破解等方式非法登录系统，对系统造成破坏，USG9500提供严格的密码安全策略，保证登录到系统的用户的合法性，最大限度保障系统安全。

2.2.3 不可否认性/Non-repudiation

不可否认性防止个人或实体否认对数据或网络执行一个具体的操作，并提供可用的证据。这些证据包括数据的起源，所有权和资源的应用等。需要确保这些证据可以呈现给第三方用以证明一些事件或操作曾经发生过。不可抵赖特性与登录，认证，授权，访问等相关安全事件均相关。

USG9500提供详细的日志审计和监控功能，日志种类包含操作日志和安全事件日志，可以记录用户登录、认证、操作等详细信息。

2.2.4 数据机密性/Data Confidentiality

数据机密性防止数据或信息未经授权的泄漏，确保数据内容无法被未经授权的实体或个人获取，加解密技术是数据机密性保护的常用机制。

USG9500 对于用户的敏感数据（如口令，证书私钥等）在设备上进行存储时都进行了加密，加密算法遵循标准，如采用AES，SHA等标准算法。

2.2.5 通信安全/Communication security

通信安全主要确保不同系统或网络之间的互访安全，需要对传输过程中的数据流提供安全保护，例如防篡改，防伪造等。

USG9500支持安全的通信协议，如SSL/TLS，SSH，SNMPv3等。

2.2.6 数据完整性/Data integrity

数据完整性用以描述确保数据、文件的完整和准确特性，防止数据、文件发生恶意篡改、替换。

2.2.7 可用性/Availability

可用性体现系统或网络在任意时刻需要和开始执行任务时，处于可工作或可使用状态的程度。可用性相关的冗余、备份等策略也是重要的安全手段。USG9500设备从硬件到部署均提供高可靠性的冗余备份能力，同时，对用户数据能够自动进行转储和备份。

2.2.8 隐私/Privacy

私密性安全纬度提供对源自对网络操作观察的信息的保护，例如当一个用户访问某一个站点，则该用户所处的地理位置、IP地址和DNS名称等信息应得到保护，防止泄漏。例如对用户信息进行加密存储、呈现匿名化。

2.3 安全面/Security Plane

各平面的融合设计，是导致网络安全问题的主要原因之一，做好三个平面的逻辑隔离和安全保护，是保护系统安全性的一个重要措施。

2.3.1 管理面/Management Plane

提供对网络设备传输设施后台支持系统（操作系统、业务系统、客户系统等）以及数据中心的故障管理、性能管理、维护等操作行为的安全保障。为了保护管理面的各种威胁，需要实现对设备和系统的安全加固，对系统进行分级授权，对配置的更改记录详细日志，对本机登陆和远程管理加强用户管理、数据传输安全和访问控制。

2.3.2 控制面/Control Plane

在网络运行过程中，为了有效进行信息传输，提供网络服务和应用，需要在网络中传输控制信息，对网络的操作行为进行控制，控制平面提供对网络控制行为的安全保护功能，包括系统组建以及和其它网元间的认证、数据的完整性、机密性等。

2.3.3 用户面/User Plane

提供对用户接入和使用网络的安全保护，实现非法用户流量的过滤，防止用户攻击流量，加强安全实时监控。

2.4 安全层/Security Layer

除了安全纬度和安全平面，安全模型还定义了三个安全层：“设备安全层”，“网络安全层”，“应用安全层”。三个安全层可以被映射到 TCP/IP OSI参考模型，如下图所示。安全纬度必须适用于网络设备和设施组的某一个层次，即安全层，依据每一层的不同弱点来确定各层的应对措施。

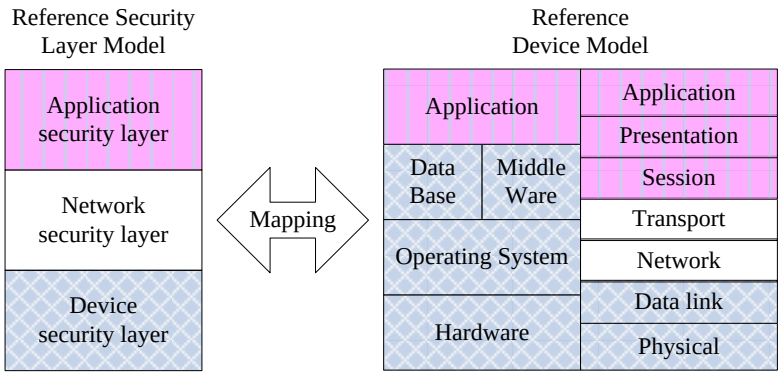


图 3 安全层与 TCP/IP OSI 参考模型的映射关系

2.4.1 设备安全层/Device Security Layer

包括各种网络传输设施和单独的网络单元，是网络和服务的基础。设备安全层所面临的挑战是实现设备和设备之间的安全通信。该层次的安全主要体现在通信线路的可靠性，如硬件、操作系统、数据库、基础协议、中间件、设备的备份、防灾害、抗干扰能力等等。该层可映射到 TCP/IP OSI 参考模型中的链路层和物理层。

2.4.2 网络安全层/Network Security Layer

主要用于为客户提供的网络服务的安全，由网络协议和逻辑网络组成。在网络安全层，我们主要聚焦在网络协议和联网的安全性，通过应用安全准则和策略，例如：深度防御、有效协同防御、安全平面分离等等来提升设备联网的安全性。网络协议的安全性涉及网络层和传输层的各种协议，如：TCP、IP、OSPF、RIP、ICMP、MPLS等。

2.4.3 应用安全层/Application Security Layer

应用安全层包含设备层和网络层的各种应用和服务以及应用的相关协议。在应用安全层，安全主要体现在各种服务和应用以及相关协议的安全，如Web应用、OM服务和应用，计费服务系统等等。应用层协议主要指会话层、表示层和应用层的协议，如：HTTP、DNS、SSH、FTP、RPC、SNMP、AAA等。

2.5 USG9500 系统安全解决方案概述

综合以上安全模型的内容，USG9500 系统从平台安全、网络安全、应用安全三个层次进行设计：

- 平台安全：包括系统加固、安全补丁等防护手段，通过提升操作系统的安全级别为 USG9500 业务应用提供安全可靠的平台。
- 网络安全：包括组网隔离、访问控制、远程维护安全等安全方案，通过安全组网对 USG9500 提供防护。
- 应用安全：包括传输安全、用户管理、日志管理、用户数据管理等方案。这些安全策略针对具体的业务应用。

后续章节将按平台安全、网络安全、应用安全的顺序描述。

3 平台安全

3.1 操作系统安全

操作系统

USG9500产品采用的安全实时操作系统是华为公司针对安全业务特性而定制开发的系统软件，满足业务对操作系统的高实时性、高可靠性、高兼容性的要求，为用户提供各种应用和管理服务。同时由于采用非通用的操作系统，能够避免通用操作系统本身易受攻击的缺点，最大限度的保证设备的安全。

只安装业务需要的软件包与服务组件，减少系统漏洞，降低系统遭受攻击风险。

使用最新或最稳定的操作系统。

系统安装时对操作系统进行安全加固，对操作系统的系统服务进行安全设置。

系统日志

记录所有与认证相关的事件；

最小化网络服务和端口开启。

端口开放必须基于服务，无用的端口默认是关闭的；

网络服务只能绑定到要提供该服务的网路接口（如SSH服务只能绑定在管理接口）。

审计日志

记录所有与认证相关的事件，包括登录错误和其他鉴权事件，帮助分析用户登录情况；

记录定时任务产生的日志；

系统的审计日志可通过VSM集中管理平台察看，同时支持发送日志和告警到第三方日志服务器和第三方网管。

系统接入、认证和授权

用户只分配完成任务的最小权限，只允许应用帐号执行应用操作；

用户登录超时时间可设置，超时后需要重新认证才能登陆。

帐号与操作环境

帐号的密码符合口令基本复杂度要求;

帐号反复尝试支持锁定，防止暴力破解。

3.2 数据库安全

USG9500使用内嵌式数据库，只对内提供接口，不对外部提供接口，保证了数据库数据不被外部所访问，也就避免了外部侵入数据库的可能性；

数据库表项数据在保存时，密码采用加密存储方式，因此即使数据库文件被恶意导出，敏感信息也不会暴露；

数据库的访问采用最小授权访问方式，仅供设备内部逻辑所调用。

4 网络安全

4.1 组网隔离

USG9500采取固定接口对外提供业务访问，数据平面与对接设备网络之间没有协议栈，不对外暴露IP，外部无法通过IP地址进行攻击。USG9500同时提供独立的带外管理接口，实现管理和业务的完全隔离。

USG9500设备可以通过设备的嵌入式 Web 环境进行单机管理，同时，产品提供了VSM集中管理平台，可用于对多台设备进行集中管理和监控。

用于单机管理的Web控制台和设备之间可以支持通过安全的HTTPS协议进行访问，VSM集中管理环境和设备之间的管理控制数据支持 SSH 协议进行加密。可以有效避免通信数据有可能被黑客窃取，造成运营商或公众客户的资料外泄。

4.2 访问控制

USG9500产品具备严格的访问控制管理，设备访问控制列表对连接设备的IP地址进行严格控制，只有经过授权的地址才能对设备进行登录、查看信息及配置等操作，同时与身份识别和认证机制结合在一起，可以有效防止非授权用户或设备的访问操作。

4.3 远程维护

USG9500支持SSH、HTTPS方式对设备进行远程维护和管理。对于文件传输，可支持sFTP等安全的文件传输协议。

同时，支持第三方网管系统对设备进行管理和监控，可选择SNMPv3协议。

5 应用安全

5.1 用户数据安全

5.1.1 用户数据保护

个人数据定义：指直接通过该数据或者结合该数据与其他的信息，可以识别出自然人的信息。包括：最终用户姓名、帐号、主叫和被叫号码、通信记录、通信时间、定位数据等。

敏感数据：具体范围取决于产品具体的应用场景，产品应根据风险进行分析和判断。典型的敏感数据包括口令、银行帐号、大批量个人数据、用户通信内容和密钥等。

对于个人数据，如果使用不当，往往会涉及个人的隐私。各国的法律在个人数据保护方面也有相关的安全要求，USG9500产品在使用用户个人数据的过程中，具备相应的保护措施。

系统符合度

USG9500不涉及公众客户的银行帐号、私人密码信息、用户姓名帐号（手机号码、IMSI、IMEI、固网上网帐号）。

USG9500产品仅记录与安全威胁相关的事件信息，尽可能减少用户个人数据的记录。发现攻击后会记录攻击事件所对应的攻击者和受害者的IP地址和端口；攻击事件报文抓取单个攻击报文的数据内容；USG9500产品的审计功能会记录URL、文件名或者IM上下线时间等内容，该类审计信息受单独的审计管理员管理控制，并进行加密保存。以上内容通过安全组网、登录认证、安全协议、权限控制保障个人数据安全。

用户数据安全方案

1、 技术措施

a) 安全通信协议：USG9500 支持安全的通信协议，包括 SSH V2、SNMP V3、HTTPS；

b) 登录认证保护：USG9500 可以通过 WEB-UI、日志访问到可能会设计个人数据的信息。登录到显示数据的 WEB 和操作系统、数据库，均需经过用户名和密码认证；

c) 权限控制：WEB-UI 支持角色、权限控制，没经过授权的用户，不能访问含个人数据，不能执行含有个人数据的功能；

2、 审计措施

a) 非查询操作均有日志记录。

3、 管理措施

a) 禁止将日志和抓包文件传出企业或运营商网络，如需访问必须经过用户允许，并开通 VPN。

5.2 认证和授权管理

5.2.1 基于角色的用户管理

使用基于角色的授权体系。帐号、角色的授权适用最小化授权原则。即：角色仅仅授予其工作所需的必要权限；帐号仅仅授予其工作所必需的必要角色。支持数据级粒度角色控制，让不同角色的用户可以执行同样的功能，但不能查看功能内部的敏感信息。确保管理、维护与操作分离。

USG9500系统支持对不同的用户分配不同的权限。除系统默认的系统管理员、操作员、审计员，系统还支持用户自定义管理员角色，根据配置管理内容以及需要管理的设备进行细粒度的定义，并授予相应权限的用户。

5.2.2 安全管理

为了防止未授权用户通过暴力破解等方式非法登录系统，对系统造成破坏，USG9500 产品提供严格的密码安全策略，保证登录到系统的用户的合法性，最大限度保障系统安全。

用户和密码策略

I. 用户强制下线

管理员可以对可疑的用户执行强制下线操作。

II. 密码复杂度

USG9500 产品建议用户的口令复杂度如下：

口令长度至少 8 个字符

口令必须至少包括下面三种字符：

－小写字母；

－大写字母；

－数字；

－特殊字符：`~!@#$%^&*()-_=+\|[{}];:'",<.>/? 和空格。

口令不能和帐号和帐号的倒序相同。

III. 口令出错锁定

当重复输入错误口令次数（默认3次，系统可设置）超过系统限制时，锁定用户；

对于口令尝试N次失败被锁定的用户，系统能够设置自动解锁时间；

用户被锁时间达到预定义时间，可自动解锁该用户。

IV. 密码禁止明文存储

对于对于管理员密码、上网用户密码，服务共享密钥、SNMP v2的团体字、SNMP v3的密码进行加密存储，口令不在系统中明文存储，在不需要还原的场景，口令使用SHA算法加密，在需要还原的场景口令使用AES算法加密。加密算法中加入了盐值提高安全性。

V. 口令使用规则

USG9500产品输入口令时，不能明文回显、WEB输入框不能拷贝；

用户只能修改自己的口令，且必须验证旧密码，管理员重置密码除外管理员除外。

空闲注销策略

USG9500系统的WEB应用客户端，支持自动注销策略。通过设置不活动周期启动终端界面自动锁定策略，当WEB在指定周期内登录用户无任何操作，会话将被注销，用户再次进行WEB操作时，需要再次输入帐号口令进行认证。

5.3 数据传输安全

5.3.1 安全传输协议

USG9500 使用一系列安全的协议和应用，保证数据传输安全

1、 WEB 应用使用 HTTPS。

2、 系统组件间连接访问默认使用 SSH v2。

3、 网管支持 SNMP v3。

4、 与外部系统进行文件传输可通过 HTTPS 或者 SFTP 操作。

5、 在线升级包等数据导入前均进行文件完整性校验。

5.4 日志管理

根据华为的日志规范，记录日志内容，日志中包含时间发生的时间、用户ID、事件类型、被访问的资源名称、事件的结果。

对日志进行定期审核，排查安全防线，排除安全隐患。

5.4.1 操作日志

操作日志是记录各用户在 USG9500的WEB客户端发起的各种操作，并将最终导致的结果记录保存，作为操作日志。用于出现故障时查看在特定时间段的操作情况，帮助维护人员定位故障。审计人员可通过Web导出和查看操作日志，定期审计操作维护人员进行的操作，及时发现不当或恶意的操作。操作日志也可作为抗抵赖的证据。

操作日志记录的范畴包含以下场景：

- 用户登录相关事件，如用户登录/退出等操作；
- 用户管理相关事件，如用户的增/删/改、口令更改、权限变更等；
- 系统管理相关事件，如对系统各参数值的增/删/改。

5.4.2 运行日志

运行日志主要用于记录系统和服务器运行情况的信息，由系统的各个业务模块产生。维护人员可通过查看运行日志，了解和分析系统的运行状况，及时发现和处理异常情况。运维人员可以导出运行日志，发送给技术支持工程师定位故障。

运行日志记录的范畴包含以下场景：

- 记录系统运行过程中的异常状态和异常动作，如配置失败等；
- 记录系统运行过程中的关键事件，如系统启动、系统关闭；
- 系统管理相关事件，如对系统各参数值的增/删/改。

5.4.3 系统日志

USG9500 的系统日志记录的范畴包含以下场景：

- 系统启动日志
- 系统资源信息（CPU、内存、温度、存储介质使用率等）
- 硬件信息
- 网口流量信息