文档密级：公开

优炫工业安全网关

UXSG

产品介绍

北京优炫软件股份有限公司

目　　录

1 产品概述

优炫工业安全网关（UXSINO Security Gateway，简称 UXSG）设备集工业协议网络交换、数据传输加密、病毒侦测、防 DoS 攻击、流量控制、内容过滤、应用程序管制、AAA 认证、IPSec VPN、IPS（Intrusion Prevention System）、IPv6 支持等诸多功能于一体的新一代工业安全网关产品。

设备集成了加密、认证、交换、防火墙等功能，最大程度的减少了故障点，增加了可靠性。并且高带宽，低时延，对用户业务影响非常小。具有部署简单，组网模式简洁，易维护，运营成本低的特点。

广泛适用于电力、石油、化工、军工、制造等各行业。

2 产品介绍

2.1 通用特性

- 高性能 ASIC 芯片设计，工业 EMC 四级标准；
- 支持-40℃～85℃工业宽温工作环境；
- 无风扇设计，表面特殊散热材料喷涂散热方式；
- 多达 26 个以太网口，光、电口可灵活配置；
- 看门狗设计防止设备死锁；
- 支持实时时钟（RTC），确保安全审计的时间精确度；
- 支持线速安全转发，时延低至 10us 以下；
- 支持白名单、黑名单功能；
- 支持自定义方式的数据报文过滤（专家模板）；
- 支持报文深度检测，深度可 456bit；
- 支持二次开发接口，有效防止私有协议泄露；
- 过滤规则可离线配置，加密下发；
- 支持多种冗余环网协议，自愈时间可达 20ms 以内；
- 支持专用监控口配置，监控所有非法报文。

2.2 UXSG2000 系列产品介绍

- **UXSG2000：工业安全交换机**

UXSG2000 除了具备全部二层以太网工业交换机以外，专为安全防护设计了专家过滤模板，从而能够实现安全规则部署，有效保护网络安全，抵制非法报文。该过滤模板非常便于用户操作，并且可以实现离线设计和配置，并可加密配置文件，充分保护客户的知识资产。

主要特性：

（1）具备工业交换机的硬件环境/机械/EMC 特性以及二层以太网交换机的全部特性；

（2）支持快速环网倒换小于 20ms；

（3）最大可支持 52G 交换容量，低时延；

（4）支持安全专家过滤模板下发；

（5）安全模板可以支持 128 条；

（6）安全规则支持最大 456bit 的用户定义规则；

（7）安全模板可以加密下发，保护用户知识资产；

（8）指定专用监控口。

● UXSG2100：工业加密安全交换机（接入端）

具备工业交换机的硬件环境/机械/EMC 特性以及二层以太网交换机的全部特性；适用于工业接入端网络设备，设备支持 SM1/4 加密，加密处理能力可以支持最多 16 路加密，带宽可达 20M，IPSec 通道业务不影响原有的交换业务开通；用于通信网络的接入层加密和交换；充分保护客户数据安全性，可以穿透 IP 可达网络，极容易部署开通业务，又实现了业务之间的隔离。

● UXSG2101：工业加密安全交换机（平台端）

具备工业交换机的硬件环境/机械/EMC 特性以及二层以太网交换机的全部特性；适用于工业平台端网络设备，设备支持 SM1/4 加密，加密处理能力可以支持最多 1024 路加密，带宽可达 300M，IPSec 通道业务不影响原有的交换业务开通；用于通信网络的平台端加密和交换；每台 UXSG2101 可以对应多台 UXSG2100 使用，充分保护客户数据安全性，可以穿透 IP 可达网络，极容易部署开通业务，又实现了业务之间的隔离。

UXSG2100 和 UXSG2101 主要特性：

（1）具备工业交换机的硬件环境/机械/EMC 特性以及二层以太网交换机的全部特性；

（2）支持快速环网倒换小于 50ms；

（3）高带宽最大可支持 26G 交换容量，低时延；

（4）支持安全专家过滤模板下发；

（5）安全模板可以支持 256 条；支持 IPSec 隧道，

（6）安全规则支持最大 456bit 的用户定义规则；

（7）安全模板可以加密下发，保护用户知识资产；

（8）指定专用监控口；

（9） 支持 SM1/4 加密，加密处理能力可以支持最多 16 路加密，带宽可达 20M。

2.3 UXSG3000 系列产品介绍

- **UXSG3000：工业安全通信网关（接入端）**

具备完整的工业防火墙特性，支持最大 512 条安全模板，处理带宽高达 1000M，同时支持 SM1~4 加密，最大可支持 16 通道数，30M 加密处理能力，进一步保护用户数据安全。用于通信网络的接入端数据加密。

- **UXSG3100：工业安全通信网关（平台端）**

具备完整的工业防火墙特性，支持最大 1K 条安全模板，处理带宽高达 8000M，同时支持 SM1~4 加密，最大可支持 1K 通道数，300M 加密处理能力，进一步保护用户数据安全。用于通信网络平台端数据加密，每台 UXSG3100 可以对应多台 UXSG3000 使用。

主要特性：

（1） 业务数据加密：IPSec VPN 隧道，支持国密 SM1/2/3/4 算法；

（2） 白名单报文深度检测：以太网 12 元组等标准协议和用户数据，以及内容、病毒应用层协议过滤；

（3） 基于策略/角色组的用户认证安全策略，提供多种认证方式如本地数据库、RADIUS、LDAP 等；

（4） CA 证书统一部署；

（5） 基于用户安全策略的参数设置；

（6） 设备自身抗攻击，并能够抵抗经过设备的各种攻击，如端口扫描、OS 探测，SYN flood 等；

（7） 入侵检测与阻拦；

（8） 通过 Syslog 提供实时入侵警告，智能日志便于审计和重放；

（9） 支持丰富的服务质量 QoS；

（10） 提供本机日志/应用日志/IDP 日志/VPN 等各种日志；

（11） 5 类管理员安全权限。

2.4 UXFW2000 系列产品介绍

- **UXFW2000：工业安全协议防火墙**

具备工业交换机的硬件环境/机械/EMC 特性以及二层以太网交换机的全部特性，具备完整的工业防火墙特性，针对 ModBus 等工业协议做了深入细化的定义和处理，支持二次开发接口，有效防止私有协议泄露。扩充了安全表项到 256，提高了安全等级和处理效率。

主要特性：

（1） 高性能 ASIC 芯片设计，工业 EMC 四级标准；

（2） 支持-40℃～85℃工业宽温工作环境；

（3） 无风扇设计，表面特殊散热材料喷涂散热方式；

（4） 多达 26 个以太网口，光、电口可灵活配置；

（5） 看门狗设计防止设备死锁；

（6） 支持实时时钟（RTC），确保安全审计的时间精确度；

（7） 支持线速度安全转发，时延低至 10us 以下；

（8） 支持白名单、黑名单功能；

（9） 支持自定义方式的数据报文过滤（专家模板）；

（10） 支持报文深度检测，深度可 456bit；

（11） 支持二次开发接口，有效防止私有协议泄露；

（12） 过滤规则可离线配置，加密下发；

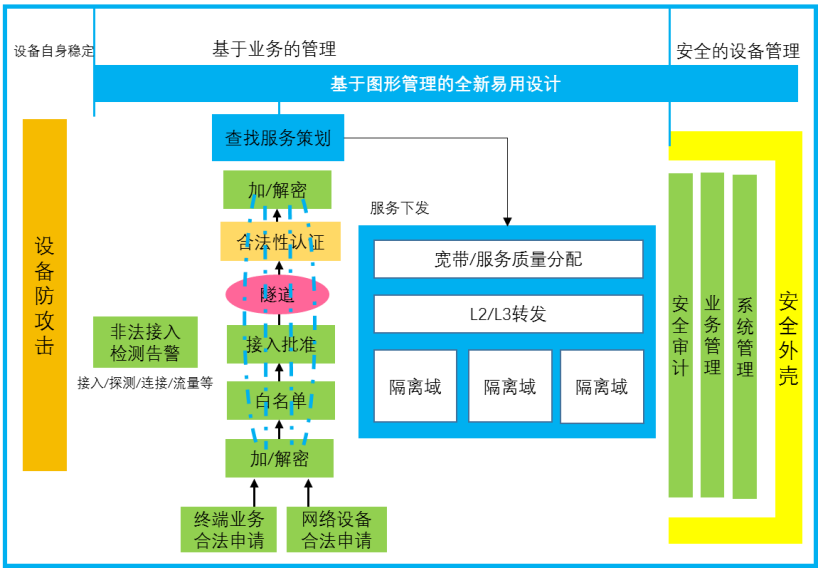
（13） 支持多种冗余环网协议，自愈时间可达 20ms 以内；

（14） 支持专用监控口配置，监控所有非法报文；

（15） 支持 ModBus 等工业协议深度定制。

3 总体技术路线


用户业务安全防护
通信设备自身防护
综合业务集成管理
易运维
数据通信
高性能、高可靠性


设备自身稳定
基于业务的管理
安全的设备管理
基于图形管理的全新易用设计
设备防攻击
查找服务策划
加/解密
合法性认证
隧道
非法接入检测告警
接入/探测/连接/流量等
接入批准
白名单
加/解密
终端业务合法申请
网络设备合法申请
服务下发
宽带/服务质量分配
L2/L3转发
隔离域
隔离域
隔离域
安全审计
业务管理
系统管理
安全外壳

4 产品核心技术

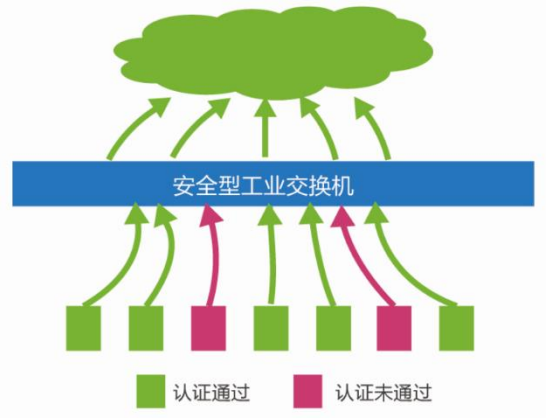
- **核心价值点 1—接入身份认证**

  功能：所有接入模块都需要经过安全型工业交换机的认证，才能允许数据通过。

  目的：在接入层初步隔离非法数据，保护网络带宽不被非法数据占用。

  认证方式 1：简单的 MAC 地址认证

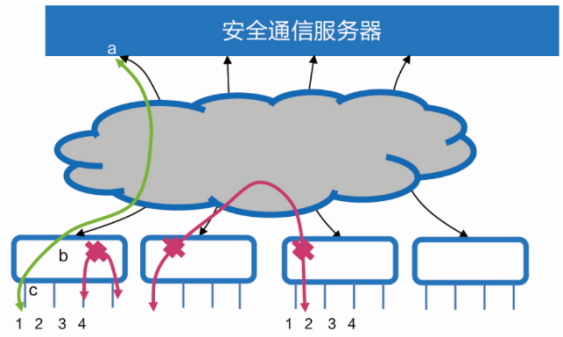
  认证方式 2：CA 证书统一部署



- **核心价值点 2—用户接入业务隔离**

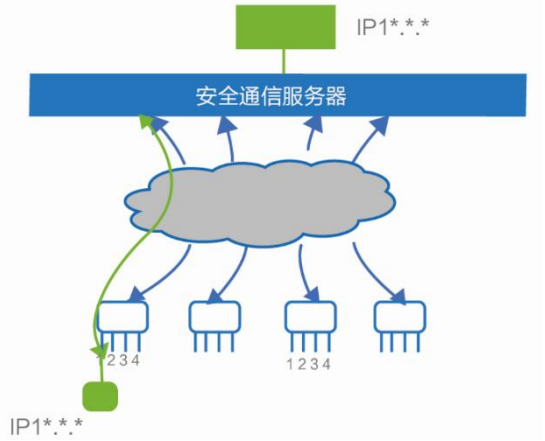
  功能：接入网的所有接入端口之间，实现物理隔离，只允许各接入端口和安全通信服务器通信。

  目的：避免异地攻击。

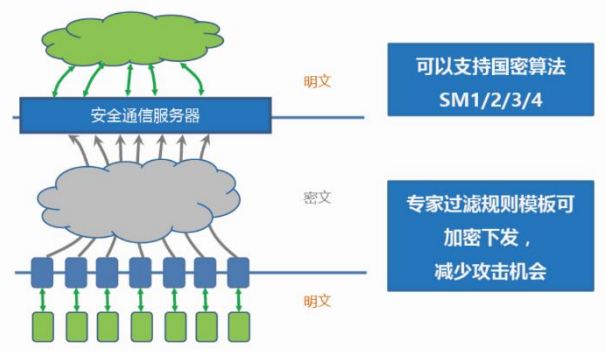


- **核心价值点 3—IPSec 业务专用通道**

  IPSec 能够为业务分配单独传输通道。



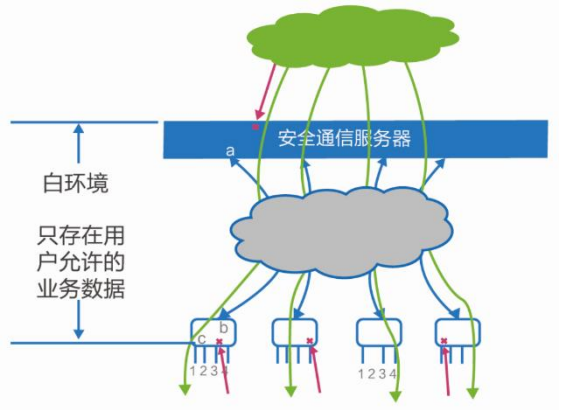
- **核心价值点 4—核心数据加密**



- **核心价值点 5—白环境，网络可靠转发**

1) 设备上电缺省不做任何转发，充分保证安全性。

2) 安全、可靠、细致的接入层业务数据转发白环境。防止了恶意数据通过，不仅保护用户设备免受非法攻击，而且能够保护用户的网络带宽资源。



- **核心价值点 6—网络设备自身防护**

1) 专用网管端口通道：专用管理口进行配置管理，减少了攻击机会，更加安全。

2) 非法报文集中监控：可以配置某端口为专用监控端口，用来监控所有非法报文。

3) 完善日志：支持非法区域穿越，用户登录，日志等安全审计功能。

4) 防攻击：设备自身支持防 DOS、端口恶意扫描、IP 欺骗等各种攻击，通信网络更健壮。

5) 管理用户权限和防护：更加完整的设备管理防护体系，从加密、口令等各个方式，进行安全防护。

6) 易运维：管理用户权限和防护、专家模板使设计与应用分离、模板离线设计，统一下发、支持模板学习模式、内置 Modbus 等标准工业协议过滤模板。

5 解决方案特点

（1）部署简单，组网模式简洁，易维护，运营成本低。

（2）设备集成了加密、认证、交换、防火墙等功能，最大程度的减少了故障点，增加了可靠性。

（3）高带宽，低时延，对用户业务影响非小。