
安防监控网络安全解决方案
西通光电网络智能科技公司

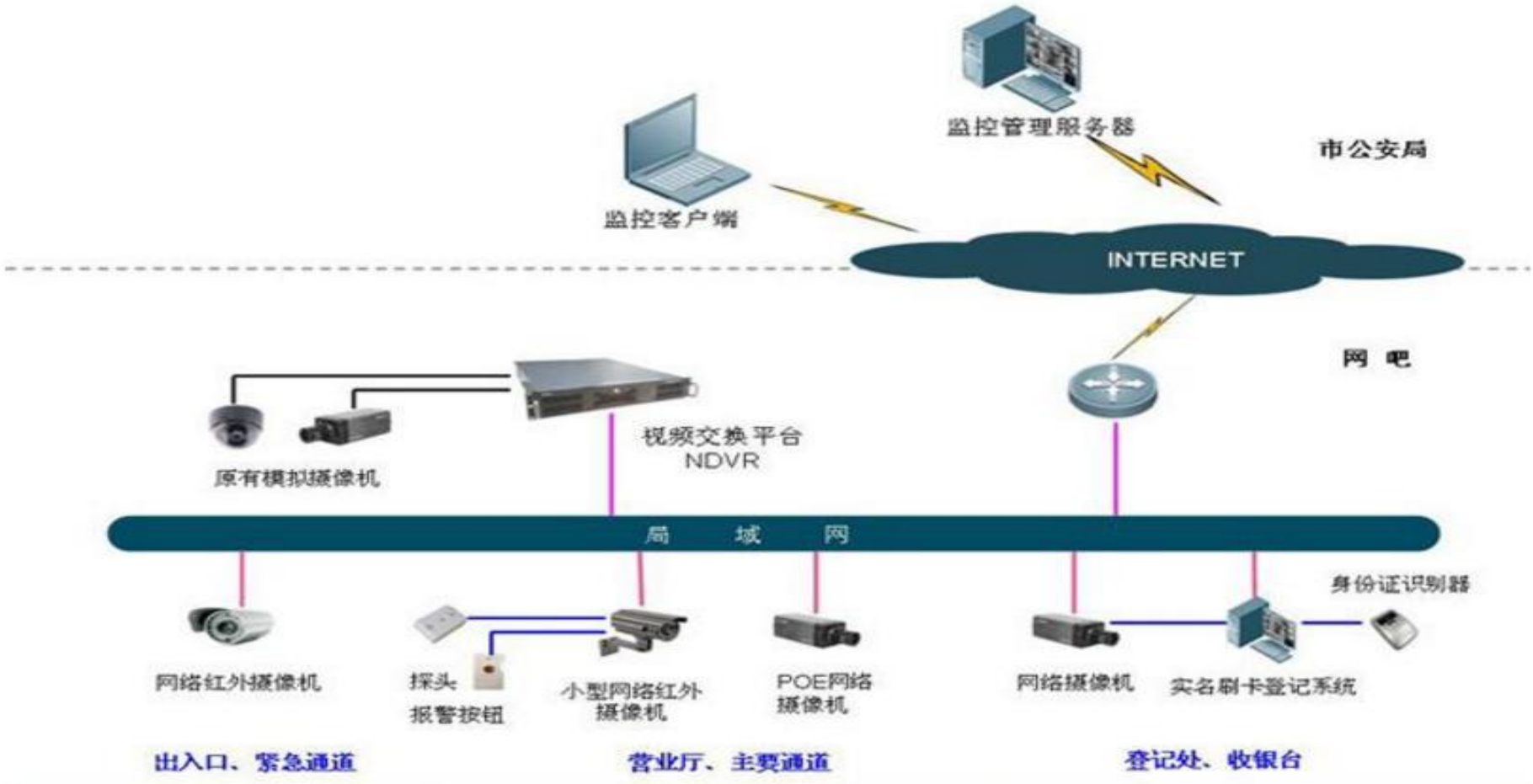
安防监控的网络安全谁来负责？！

- **视频接入安全网关系统**，是基于视频监控应用场景开发的一款网络安全产品。
- 该产品旨在为用户**提供全方位的摄像头、服务器安全防护，防私接/替换，防网络攻击，保证视频流单向通过，保障视频监控网络的安全。可串接、旁路部署。**

适用于：**公安，教育，小区等部署视频监控并有安全需求的场所**

应用场景概述

- 网络摄像头：采用 TCP/IP 协议传输数据和进行管理控制。
- NVR：网络硬盘录像机，对视频进行存储、管理、展示。
- 监控客户端：远程访问 NVR 服务器或网络摄像头监控画面。


监控管理服务器
市公安局
监控客户端
INTERNET
网 吧
视频交换平台
NDVR
原有模拟摄像机
局 域 网
身份证识别器
网络红外摄像机
探头
报警按钮
小型网络红外
摄像机
POE网络
摄像机
网络摄像机
实名刷卡登记系统
出入口、紧急通道
营业厅、主要通道
登记处、收银台

视频监控概述

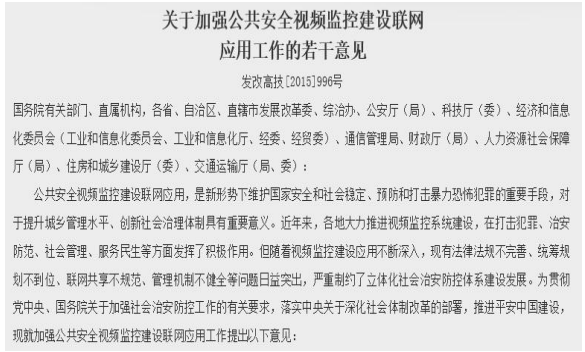
- 监控摄像头主要厂家：
  - 海康威视、大华、天地伟业、宇视。
- 控制协议：
  - ONVIF：行业标准、国际标准。致力于通过全球性的开放接口标准来推进网络视频在安防市场的应用，接口标准将确保不同厂商生产的网络视频产品具有互通性。ISG主要采用这个协议来识别和获取网络摄像头品牌，型号，序列号等特征信息。
  - GB28181：国内标准，在全国范围内的平安城市项目建设中被普遍推广应用标准。
- 视频协议：
  - RTSP：用来控制声音或影像的多媒体串流协议，并允许同时多个串流需求控制，传输时所用的网络通讯协定并不在其定义的范围内，服务器端可以自行选择使用

TCP 或 UDP 来传送串流内容，它的语法和运作跟 HTTP 1.1 类似，但并不特别强调时间同步，所以比较能容忍网络延迟。

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://www.w3.org/2003/05/soap-envelope" xmlns:SOAP-ENC="http://
www.w3.org/2003/05/soap-encoding" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:wsa="http://
schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:tns="http://schemas.xmlsoap.org/ws/2005/04/discovery"
xmlns:dn="http://www.onvif.org/ver10/network/wsdl" xmlns:wsa5="http://www.w3.org/2005/08/addressing"><SOAP-
ENV:Header><tns:AppSequence MessageNumber="10088" InstanceId="1"></tns:AppSequence><wsa:MessageID>urn:uuid:
00010010-0001-1020-8000-48ea6324fd0f</wsa:MessageID><wsa:RelatesTo>urn:uuid:15706d68a-1dd2-11b2-
a105-010203040506</wsa:RelatesTo><wsa:To SOAP-ENV:mustUnderstand="true">urn:schemas-xmlsoap-org:ws:
2005:04:discovery</wsa:To><wsa:Action SOAP-ENV:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2005/04/
discovery/ProbeMatches</wsa:Action></SOAP-ENV:Header><SOAP-
ENV:Body><tns:ProbeMatches><tns:ProbeMatch><wsa:EndpointReference><wsa:Address>urn:uuid:
00010010-0001-1020-8000-48ea6324fd0f</wsa:Address></
wsa:EndpointReference><tns:Types>dn:NetworkVideoTransmitter</tns:Types><tns:Scopes>onvif://www.onvif.org/
Profile/Streaming onvif://www.onvif.org/type/video_encoder  onvif://www.onvif.org/type/ptz  onvif://
www.onvif.org/type/audio_encoder  onvif://www.onvif.org/location/  onvif://www.onvif.org/name/UNIVIEW
onvif://www.onvif.org/macaddr/48ea6324fd0f  onvif://www.onvif.org/version/IPC_Q1201-B5012P01D1512  onvif://
www.onvif.org/serial/210235C1XSA161000017  onvif://www.onvif.org/hardware/HIC2621DE-CZFW-U  onvif://
www.onvif.org/type/IPC  onvif://www.onvif.org/register_status/offline  onvif://www.onvif.org/register_server/
0.0.0.0:5060  onvif://www.onvif.org/regist_id/24-FD-0F  </tns:Scopes><tns:XAddrs>http://192.168.0.13:80/
onvif/device_service</tns:XAddrs><tns:MetadataVersion>1</tns:MetadataVersion></tns:ProbeMatch></
tns:ProbeMatches></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

应用场景概述

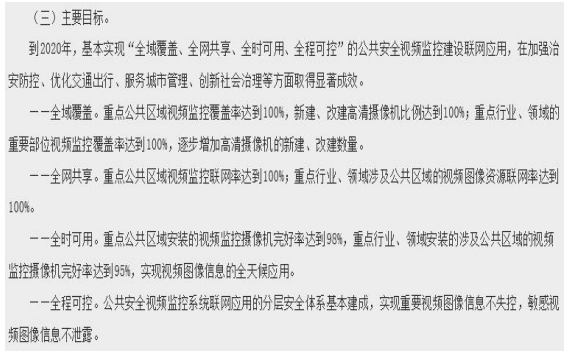
图1 某工厂摄像头漏洞利用后可以远程通过视频对工厂进行监控


关于加强公共安全视频监控建设联网
应用工作的若干意见

发改高技[2015]996号

国务院有关部门、直属机构，各省、自治区、直辖市发展改革委、综治办、公安厅（局）、科技厅（委）、经济和信息化委员会（工业和信息化委员会、工业和信息化厅、经委、经贸委）、通信管理局、财政厅（局）、人力资源社会保障厅（局）、住房和城乡建设厅（委）、交通运输厅（局、委）：

公共安全视频监控建设联网应用，是新形势下维护国家安全和社会稳定、预防和打击暴力恐怖犯罪的重要手段，对于提升城乡管理水平、创新社会治理体制具有重要意义。近年来，各地大力推进视频监控系统建设，在打击犯罪、治安防范、社会管理、服务民生等方面发挥了积极作用。但随着视频监控建设应用不断深入，现有法律法规不完善、统筹规划不到位、联网共享不规范、管理机制不健全等问题日益突出，严重制约了立体化社会治安防控体系建设发展。为贯彻党中央、国务院关于加强社会治安防控工作的有关要求，落实中央关于深化社会体制改革的部署，推进平安中国建设，现就加强公共安全视频监控建设联网应用工作提出以下意见：


（三）主要目标。

到2020年，基本实现“全域覆盖、全网共享、全时可用、全程可控”的公共安全视频监控建设联网应用，在加强治安防控、优化交通出行、服务城市管理、创新社会治理等方面取得显著成效。

——全域覆盖。重点公共区域视频监控覆盖率达到100%，新建、改建高清摄像机比例达到100%；重点行业、领域的重要部位视频监控覆盖率达到100%，逐步增加高清摄像机的新建、改建数量。

——全网共享。重点公共区域视频监控联网率达到100%；重点行业、领域涉及公共区域的视频图像资源联网率达到100%。

——全时可用。重点公共区域安装的视频监控摄像机完好率达到98%，重点行业、领域安装的涉及公共区域的视频监控摄像机完好率达到95%，实现视频图像信息的全天候应用。

——全程可控。公共安全视频监控系统联网应用的分层安全体系基本建成，实现重要视频图像信息不失控，敏感视频图像信息不泄露。

央视和国家信息安全漏洞共享平台相继报道摄像头的漏洞和入侵问题

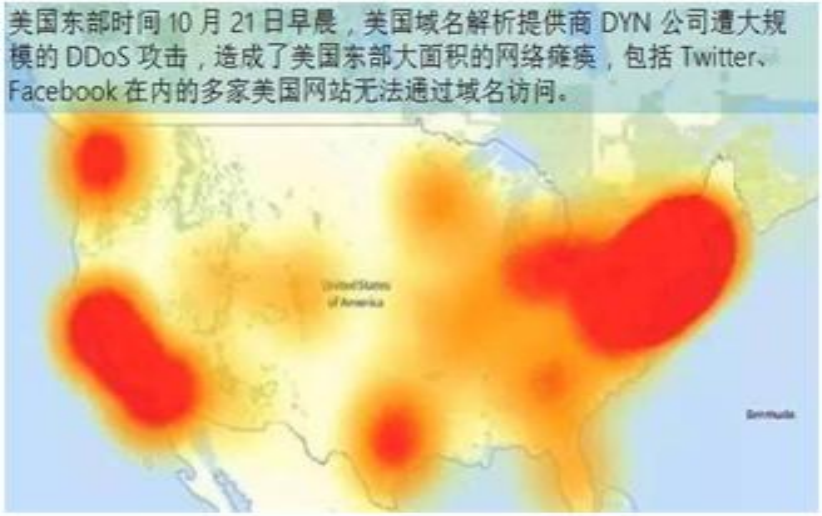
国家出台公共视频

监控的建设标准

应用场景概述

Mirai蠕虫病毒：通过病毒感染存在漏洞的物联网设备，包括：网络监控摄像头、DVR、家用路由器、智能开关等，通过远程控制成千上万的“僵尸”设备，针对攻击目标发起定向攻击；

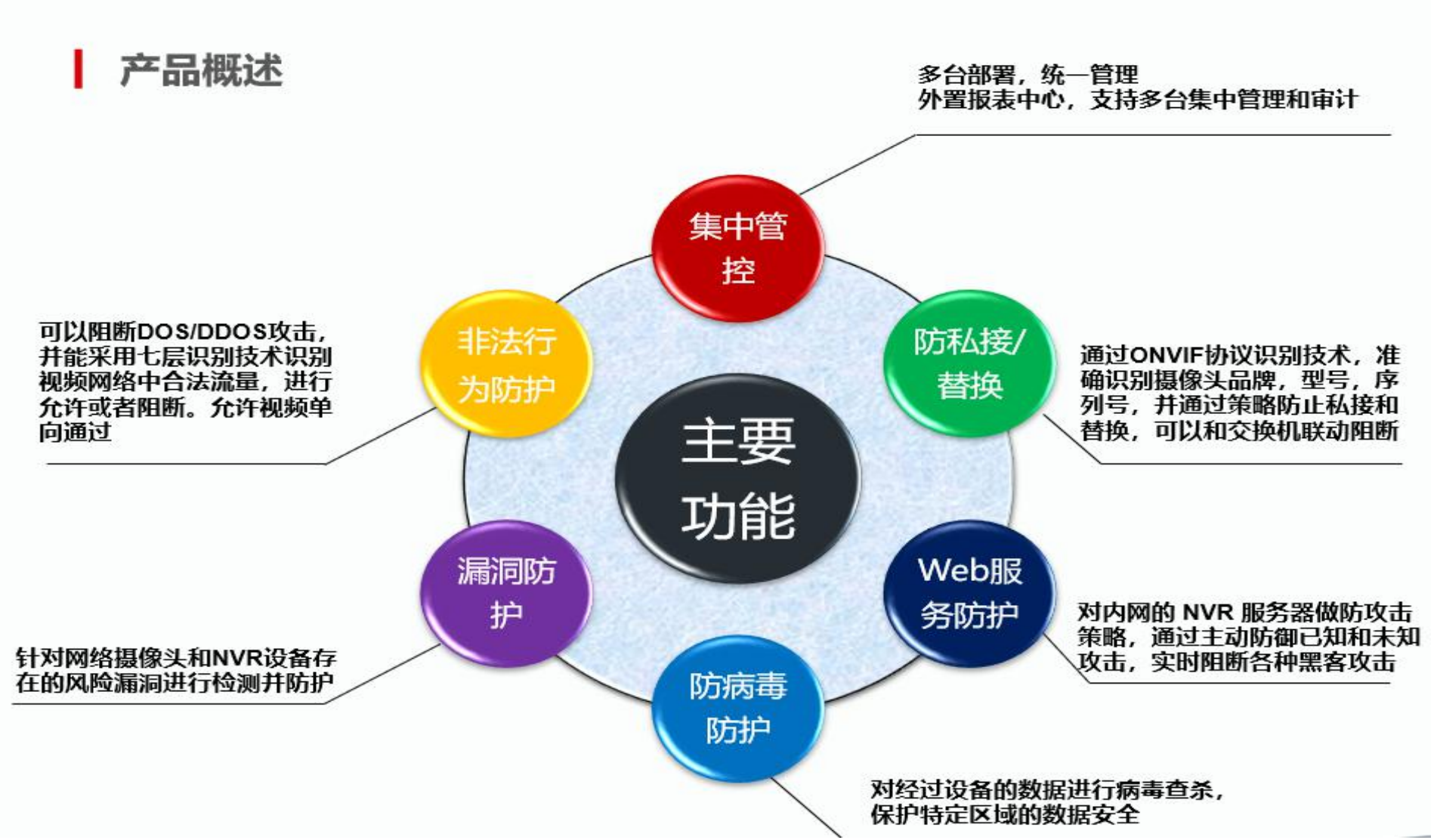
2016年10月美国东部DDoS攻击，至少上百万台设备参与了此次攻击，包括Amazon、Twitter等知名公司网站遭受攻击；Mirai会采用telnet基于数十种通用登录凭证，进行暴力破密设备；



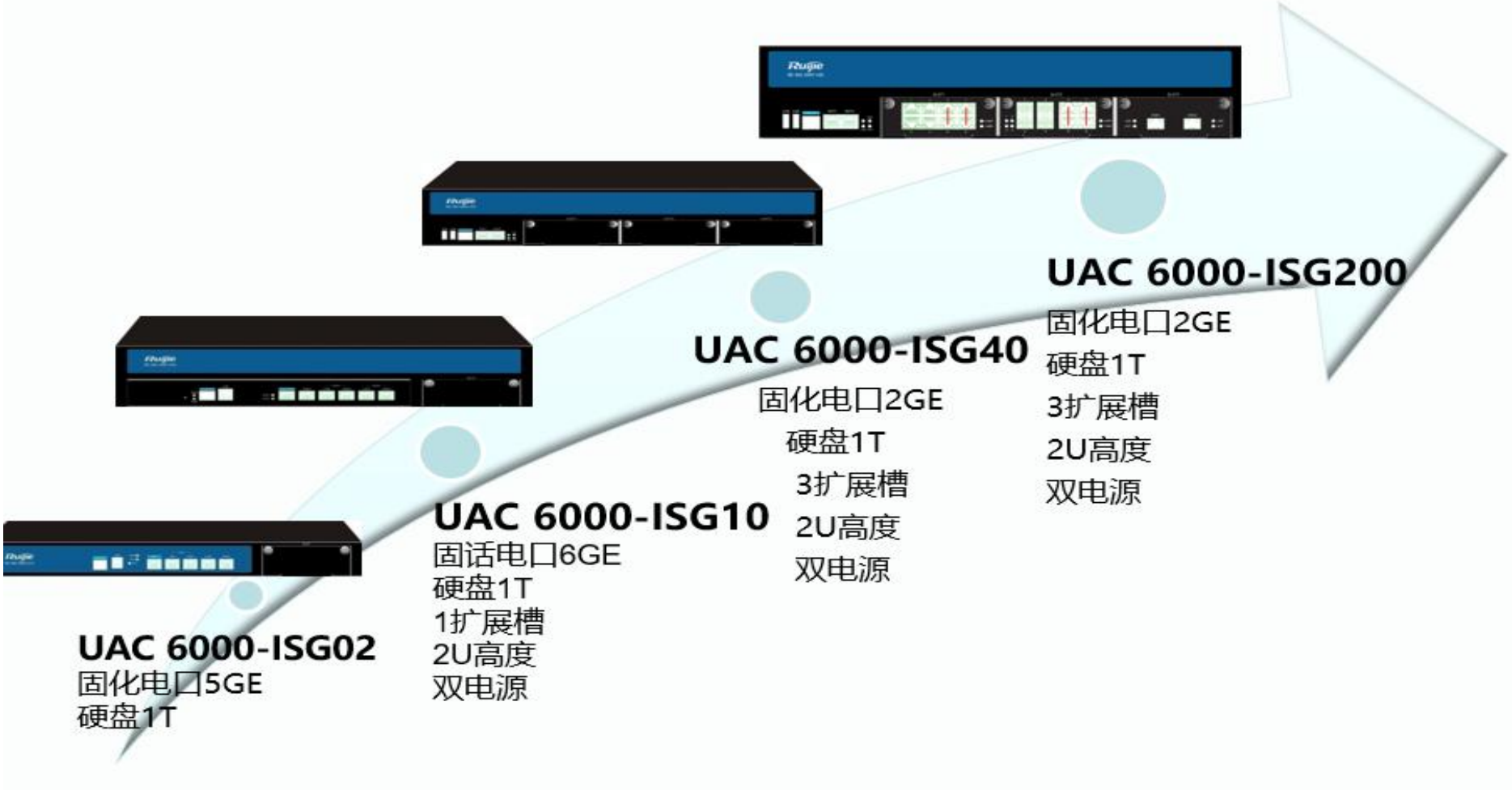
应用场景概述

- 摄像头系统的弱口令，系统自身默认的口令容易被黑客掌握；
- 拆除一个摄像头，替换为终端设备，就可以登录到监控网络中；
- 存在不必要的远程服务，厂商设备初厂时，配置了大量的开放远程服务接口，用于系统的开发和维护，上线之后，并没有合理的关闭，比如非安全的telnet,http,ftp,snmp等；
- 系统组件和应用程序漏洞，大量的开源的系统和中间件，这些基本的系统组件存在大量的安全漏洞。

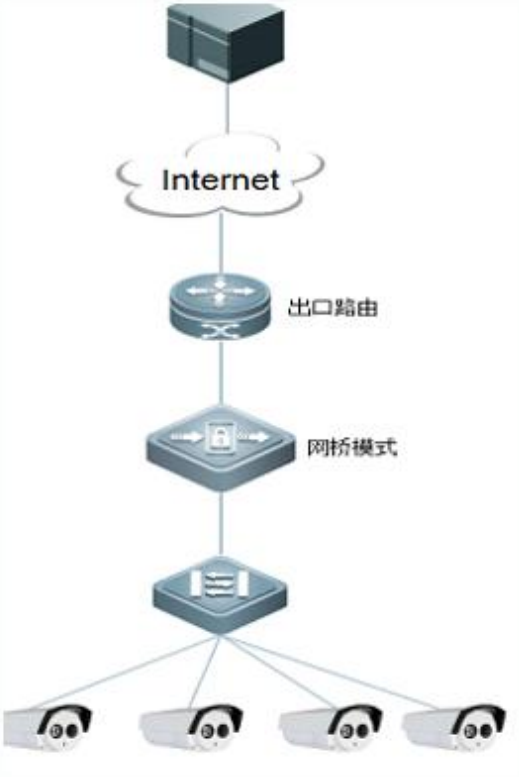
产品概述


多台部署，统一管理
外置报表中心，支持多台集中管理和审计
集中管控
可以阻断DOS/DDOS攻击，并能采用七层识别技术识别视频网络中合法流量，进行允许或者阻断。允许视频单向通过
非法行为防护
防私接/替换
通过ONVIF协议识别技术，准确识别摄像头品牌，型号，序列号，并通过策略防止私接和替换，可以和交换机联动阻断
主要功能
漏洞防护
针对网络摄像头和NVR设备存在的风险漏洞进行检测并防护
Web服务防护
对内网的 NVR 服务器做防攻击策略，通过主动防御已知和未知攻击，实时阻断各种黑客攻击
防病毒防护
对经过设备的数据进行病毒查杀，保护特定区域的数据安全

产品形态


UAC 6000-ISG200
固化电口2GE
硬盘1T
3扩展槽
2U高度
双电源
UAC 6000-ISG40
固化电口2GE
硬盘1T
3扩展槽
2U高度
双电源
UAC 6000-ISG10
固话电口6GE
硬盘1T
1扩展槽
2U高度
双电源
UAC 6000-ISG02
固化电口5GE
硬盘1T

典型组网模式



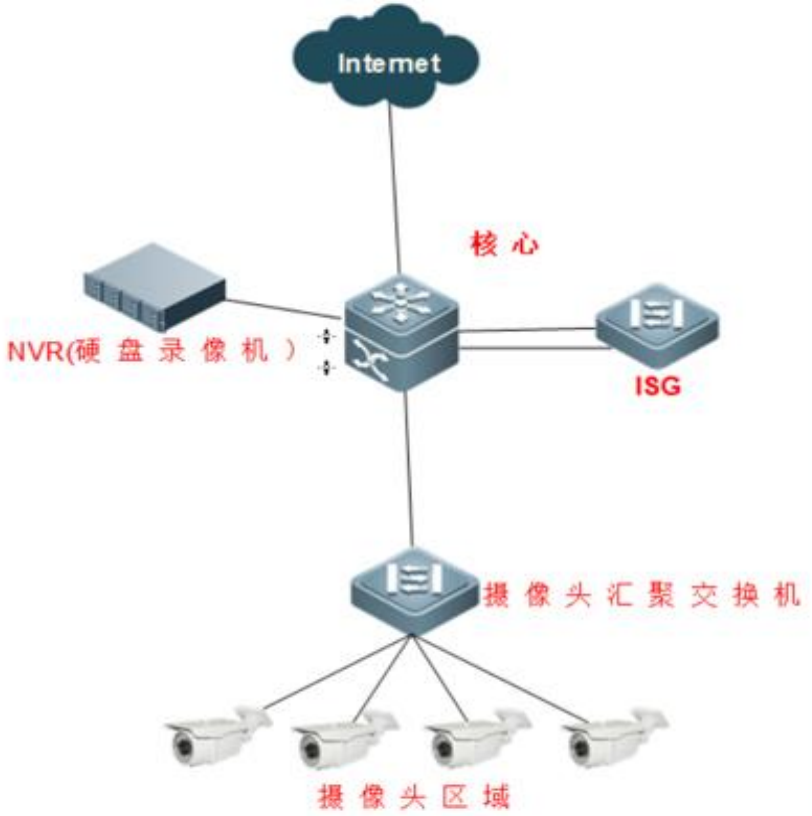
应用场景：架设在摄像头和NVR之间，监控和防止摄像头私接、替换。同时保护互联网区域非法用户针对摄像头的攻击行为；

常用功能：透明接入，不改变原有的网络结构，可靠保障摄像头安全。开启防止私接/替换，防止非法行为和攻击。只允许单向视频流通过。

设备选型：UAC 6000-ISG02/ISG10/ISG40/ISG200

典型组网应用

- **应用场景**：旁挂在网络里面，将摄像头流量镜像给ISG
- **常用功能**：发现私接/替换终端，以及非法行为，产生日志告警，交换机联动阻断私接/替换终端
- **设备选型**： UAC 6000-ISG02/ISG10/ISG40/ISG200




共享 开放 绿色 创新 协调
汇报完毕 欢迎交流
西通光电，行业信息化服务商
www.sogci.com
029-85792868 029-88856781
西安.玉祥门.天朗蔚蓝机电广场三层