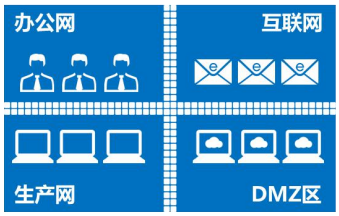
数据中心安全域隔离解决方案

数据中心安全建设的基本原则：按照不同安全等级进行区域划分，进行层次化、有重点的保护，通过传统防火墙分级分域的进行有针对性的访问控制、安全防护。



分区分域的安全管理思路
以防火墙为核心进行安全域划分

数据中心安全域隔离存在的问题

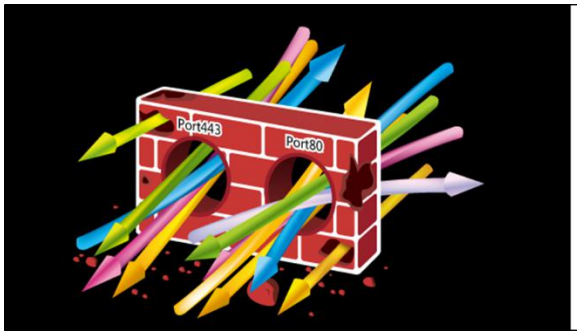
防火墙基于五元组部署访问控制策略，但仍在上线部署、业务新增和日常管理中存在策略管理复杂可视性差的问题：

全过程：管理复杂、可视性差

上线部署	业务新增	运维管理
中等规模的数据中心ACL策略可能有几百到上千条 40%的安全事件因为安全策略配置不当	业务新增快要求策略新增频繁业务变更多产生无效策略 传统墙无法感知资产新增或者变更的情况，导致策略调整浪费精力	可视性差很难判断策略用于哪些系统或者访问规则 策略不敢轻易调整，如果调整反而容易影响业务，无效策略影响防火墙性能

传统防火墙仍面临新的安全挑战

70%的攻击来自应用层，防火墙防护存在短板



- 根据Gartner的报告，用户面临的网络攻击中75%来自应用层
- 数据中心虽然划分了安全域，但在应用层攻击防护上存在明显的短板

APT、0day、欺诈等威胁出现，使边界防御失陷

- RSA认为2014年-2015年安全防御几乎“失陷”
- 各类0Day攻击、APT攻击、欺诈等高级威胁可绕过数据中心防火墙，使数据中心防御“失陷”
- 边界的防御基于静态特征，防护外到内攻击，缺乏持续对失陷主机进行持续检测的能力，导致数据中心存在大量被控制的主机也无法察觉

深信服数据中心安全域隔离解决方案

本方案采用技术上先进的下一代防火墙作为数据中心安全域隔离的主要载体。既可以解决传统安全域隔离可视性和管理便利性上的问题，同时还能够通过开启应用层防护的模块和失陷主机检测的模块加固数据中心的安全。有效的补数据中心存在的安全短板，提升数据中心安全防护与检测的能力。

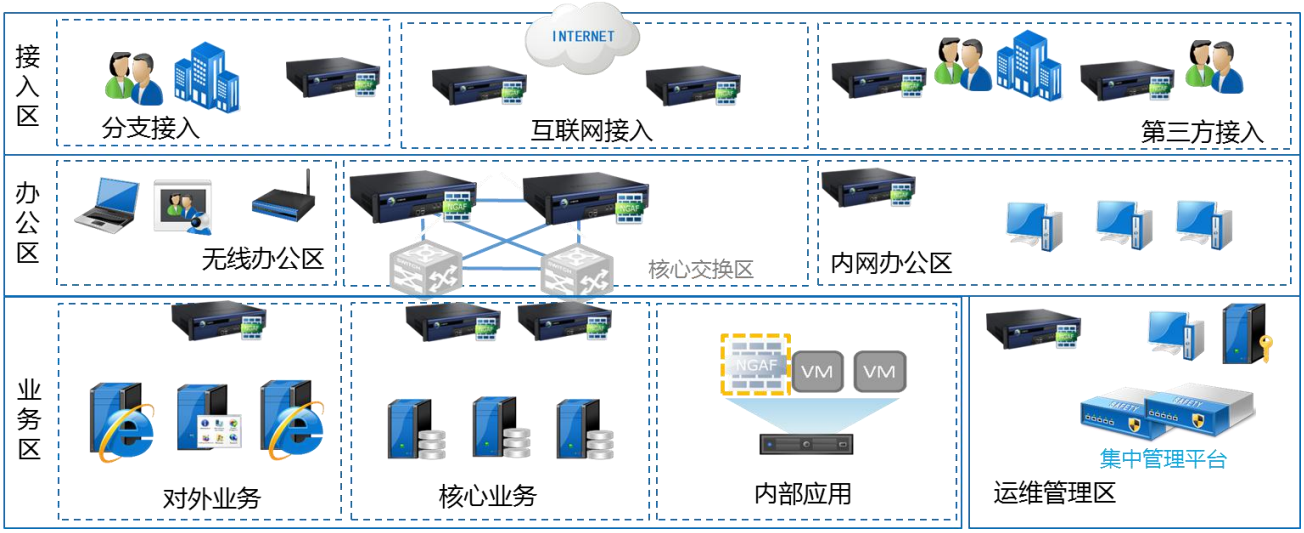
以下一代防火墙为核心

- 满足安全域划分的要求
- 精细到应用的访问控制粒度
- 向导式可视化的策略管理
- 支持更强防护和检测能力的扩展

弥

➢ 数据中心安全域设计建议

将数据中心以不同安全级别及功能需求划分为四大安全区域:接入区、办公区、业务区、运维管理区。对数据中心网络及应用系统实施网络分级分区防护，有效地增加了重要应用系统的安全防护纵深，使得外部的侵入需要穿过多层防护机制，不仅增加恶意攻击的难度，还为主动防御提供了时间上的保证。



接入区:安全等级中，包含三个子区，互联网接入区、分支机构接入区和第三方接入区；

办公区:安全等级低，包含两个子区，内网办公区和无线办公区；

业务区:安全等级高，包含三个子区，对外业务区、核心业务区、内部应用区。

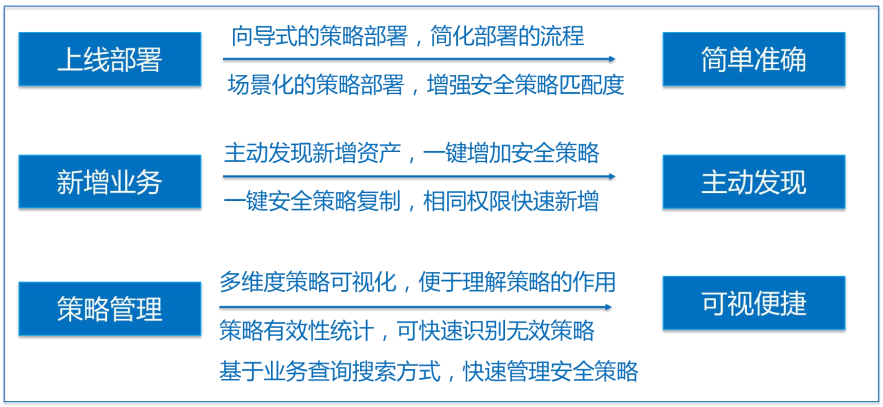
方案特点

➢ 精细到应用的访问控制粒度

不仅具备五元组访问控制策略，还可以通过结合应用识别与用户识别技术制定的 L3-L7 一体化应用控制策略,提高了策略控制的准确度，提升数据中心管理的效率。

如访问数据中心的常见应用 OA、ERP、Web、邮箱等；或外部运维人员访问数据库等场景，通过应用层访问控制策略，解决传统 ACL 的无法对端口逃逸、端口跳跃等（如使用 Oracle 建立连接 1521，连接后为随机端口）技术的应用进行控制的问题。

➢ 向导式可视化的策略管理



上线部署：简单易懂的 IT 向导配置，无需管理员掌握复杂的安全知识，也可以完成策略的快速部署上线，轻松掌握对数据中心安全策略的部署。

新增业务：数据中心新增业务时，能主动发现新增资产，防止安全策略疏漏。管理员无需手动查找新增资产，只需要对新增资产进行一键策略的关联部署就可以快速添加策略。

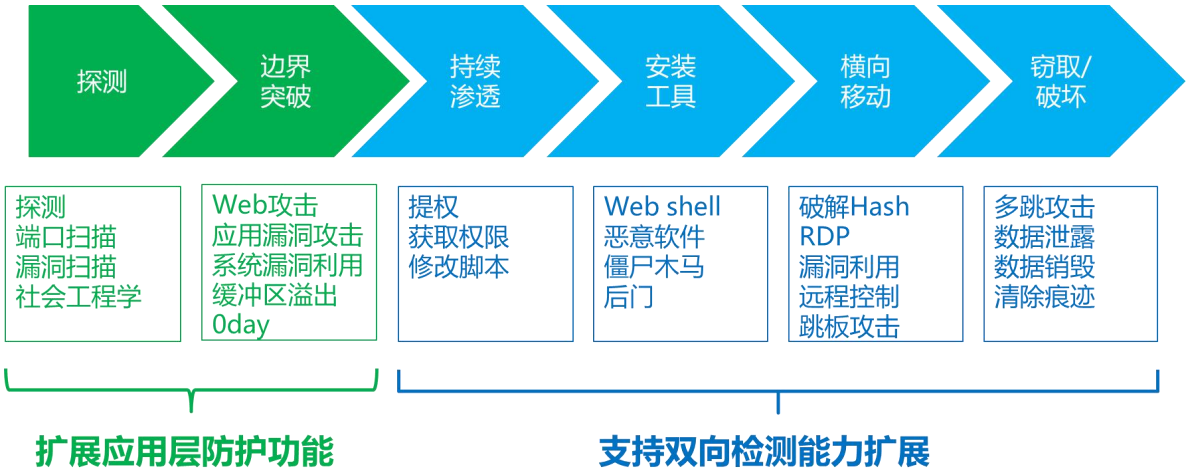
策略管理：可视化的策略管理，提升了访问控制策略管理的可视性，使管理员可以更容易的看清楚策略部署的情况；同时提供策略命中数量，便于管理员清除无效策略。

➢ 支持更强防护和检测能力的扩展

L2-7 层防护功能扩展：本方案采用深信

服下一代防火墙，可以通过开启多种防护模块对数据中心应用层防护进行安全加固。既实现了数据中心 L2-7 层完整的安全防御体系的建设，满足高性能、高可靠要求，同时解决了数据中心部署多台安全设备带来的单点故障、性能消耗、难以管理的问题。

双向检测能力扩展：本方案还可以开启失陷主机检测的模块，通过双向的行为检测技术，对数据中心服务器以及终端的外发流量进行多个维度的安全检测，可帮助管理员及时发现数据中心的失陷主机，防止由于边界被突破带来的安全风险。



数据中心用户案例

国土资源部：在数据中心服务器区和内网办公区前端分别部署了深信服下一代防火墙。替换原有的 UTM、防病毒网关、IPS、IDS 等传统网络安全设备，简化了组网拓扑，便于维护网络的稳定性。开启应用层防护功能，能实时检测数据中心否存在安全风险，为国土资源部的网络提供强有力的安全保障。

招商局集团：2012 年建成一个模块化设计架构的 IDC 数据中心。安全方面，在数据中心 DMZ 区、业务数据区等多个区域部署了数十台万兆下一代防火墙 NGAF。不仅仅进行了安全域划分，并为各业务系统提供了 L2-7 层完整的安全防护。在可靠性保障方面，通过单次解析架构、多核并行处理技术实现了万兆级别的应用层处理性能，有效保障数据中心高可靠的要求。

国家信息中心	工信部	国美电器集团	招商银行	顺义教育信息中心
国土资源部	卫生部	招商局集团有限公司	申银万国证券	兴业银行河北省分行
公安部	环保部	中国南车集团	保监会	中国电信集团