



Hyper scan在X86防火墙产品中的 应用实践

2017.3.8

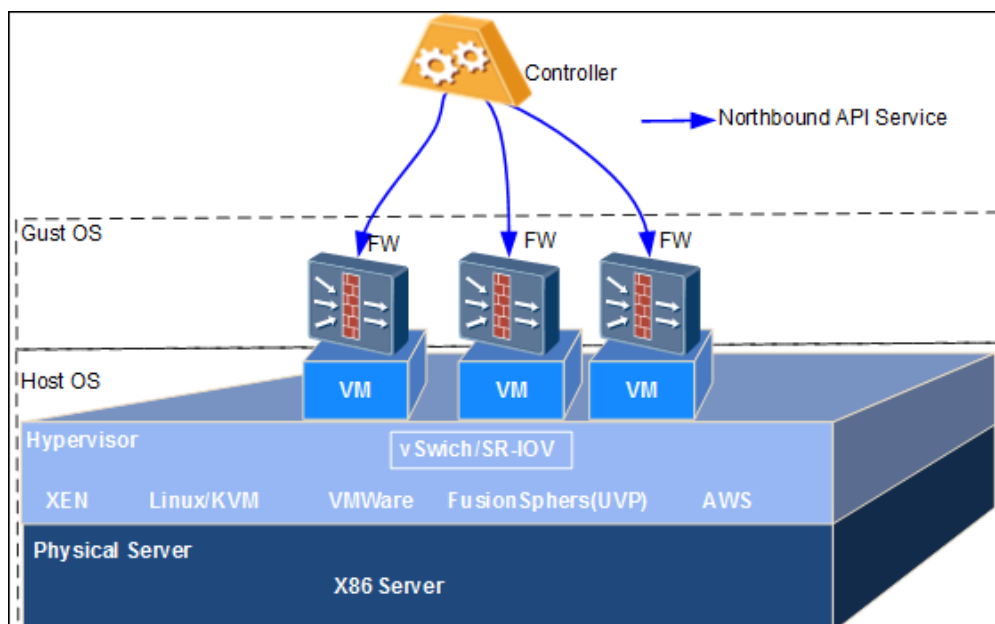
www.huawei.com



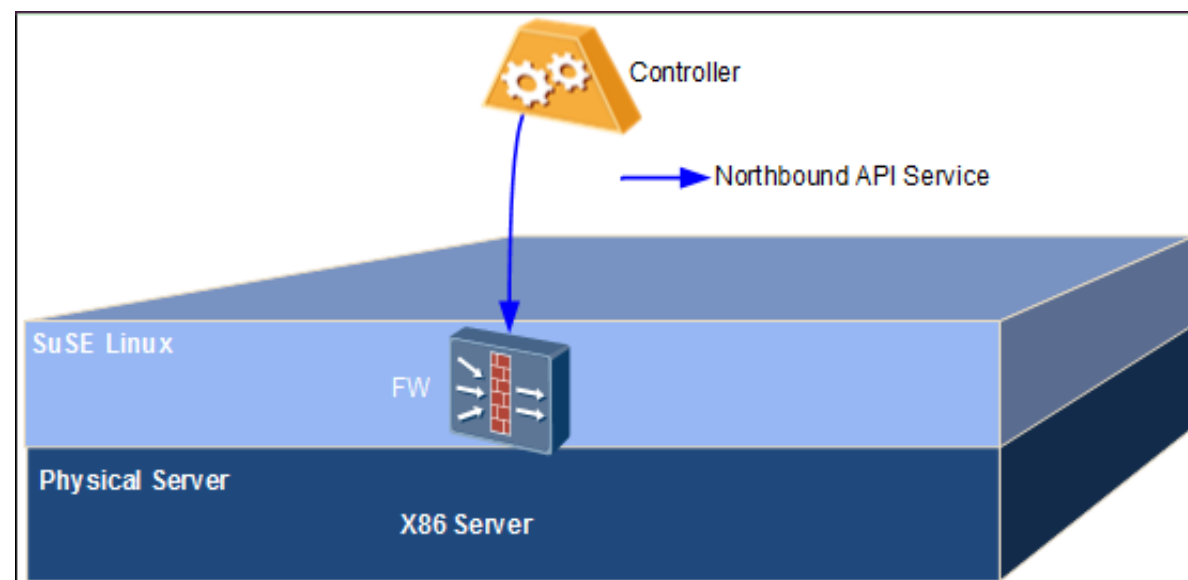
- x86防火墙产品简介
- hyperscan的使用
 - 模式编译
 - Database管理
 - 模式匹配
- hyperscan相关诉求汇总

x86防火墙产品简介

华为x86防火墙产品可运行在标准服务器虚拟机上，面向云数据中心及NFV场景，提供全面软件化部署的虚拟网络安全防护。通过软件定义安全来实现安全能力的快速部署。



虚拟化平台部署



X86服务器部署

x86防火墙产品简介

首页 > 产品 > 安全 > 防火墙及应用安全网关 > USG6000V

USG6000V 虚拟综合业务网关

华为USG6000V(Universal Service Gateway)是基于NFV架构的虚拟综合业务网关，虚拟资源利用率高，资源虚拟化技术支持大量多租户共同使用。产品具备丰富的网关业务能力，如vFW、vIPSec、vLB、vIPS、vAV、vURL过滤等，可根据对虚拟网关的业务需求，按需使用，灵活部署。

USG6000V系列虚拟综合业务网关兼容多种主流虚拟化平台，提供标准的API接口，可以与华为FusionSphere云平台、Agile Controller控制器以及开源的Openstack平台共同构成开放的SDN数据中心解决方案。USG6000V可以与传统硬件设备统一被Agile Controller控制器进行管理，构建统一的智能化云安全平台，实现业务灵活定制，资源弹性扩缩，网络可视化管理，满足企业业务快速上线、变化频繁，运维简单、高效等诉求。



USG6000V



<http://e.huawei.com/cn/products/enterprise-networking/security/firewall-gateway/usg6000v>

提纲

- USG6000V产品简介
- hyperscan的使用
 - 模式编译
 - Database管理
 - 模式匹配
- hyperscan相关诉求汇总

hyperscan的使用

●使用场景

- ✓DPI应用识别
- ✓IPS检测
- ✓关键字扫描

●软硬件环境

CPU: X86

业务多线程工作模式

●Hyperscan版本

V4.3.0

libhs.so

模式编译

●规则集编译

Pattern属性: HS_FLAG_CASELESS
HS_FLAG_SOM_LEFTMOST

编译模式: HS_MODE_STREAM
HS_MODE_STREAM + HS_MODE_SOM_HORIZON_SMALL

Pattern规模: 20K+

模式编译

●编译资源占用

database大小: 16MByte (pattern数目7000+)

编译时间: < 25s

峰值内存: 100+MByte

Database管理

- 规则集尽可能多的拆分成独立的database
- 尽量采用EOM的编译模式
- 各线程独立的scratch空间，用于db更新切换

```
hs_error_t hs_alloc_scratch(const hs_database_t *db, hs_scratch_t **scratch);
```

缺点：Db越多， scratch空间占用越多。

模式匹配

- 多线程匹配

各线程独立的scratch空间;

```
hs_error_t hs_alloc_scratch(const hs_database_t *db, hs_scratch_t **scratch);
```

- 流模式，跨包匹配

```
hs_error_t hs_scan_stream(hs_stream_t *id, const char *data,  
                          unsigned int length, unsigned int flags,  
                          hs_scratch_t *scratch, match_event_handler onEvent,  
                          void *ctxt);
```

跨包缓存大小无法设置;

●多线程匹配性能

| 吞吐量单位：Mbps（单核） | | | | |
|----------------|------------|------------|------------|------------|
| db \ payload | pattern-01 | pattern-02 | pattern-03 | pattern-04 |
| payload01 | 335 | 1061 | 1188 | 2263 |
| payload02 | 514 | 1541 | 1000 | 2738 |
| payload03 | 549 | 1904 | 836 | 11055 |
| payload04 | 472 | 1397 | 1126 | 2361 |
| payload05 | 368 | 1108 | 1082 | 4183 |
| payload06 | 466 | 1353 | 1046 | 5794 |

| 吞吐量单位：Mbps（10核） | | | | |
|-----------------|------------|------------|------------|------------|
| db \ payload | pattern-01 | pattern-02 | pattern-03 | pattern-04 |
| payload01 | 3388 | 10469 | 11450 | 22324 |
| payload02 | 5210 | 15328 | 9514 | 27064 |
| payload03 | 5558 | 17935 | 7759 | 108199 |
| payload04 | 4805 | 13245 | 10648 | 23150 |
| payload05 | 3760 | 10960 | 10482 | 40517 |
| payload06 | 4721 | 13530 | 9809 | 55254 |

| 多核性能线性度 | | | |
|------------|------------|------------|------------|
| pattern-01 | pattern-02 | pattern-03 | pattern-04 |
| 10.11 | 9.87 | 9.64 | 9.86 |
| 10.14 | 9.95 | 9.51 | 9.88 |
| 10.12 | 9.42 | 9.28 | 9.79 |
| 10.18 | 9.48 | 9.46 | 9.81 |
| 10.22 | 9.89 | 9.69 | 9.69 |
| 10.13 | 10.00 | 9.38 | 9.54 |

提纲

- USG6000V产品简介
- hyperscan的使用
 - 模式编译
 - Database管理
 - 模式匹配
- hyperscan相关诉求汇总

hyperscan相关诉求汇总

- 编译峰值内存占用

与pattern规模的关系?

峰值内存估算方法?

- 匹配内存占用

scratch空间大小可以查看, stream空间大小查看?

除了scratch和stream以外, 其它的内存占用?

单条流的stream大小占用优化?

hyperscan相关诉求汇总

●Database切换

每一个线程创建一个scratch空间, db更新后, scratch是否必须更新?

●匹配相关

- 1) 命中结果的最大个数限制、配置;
- 2) 指定多个database 匹配;



Thank You

www.huawei.com