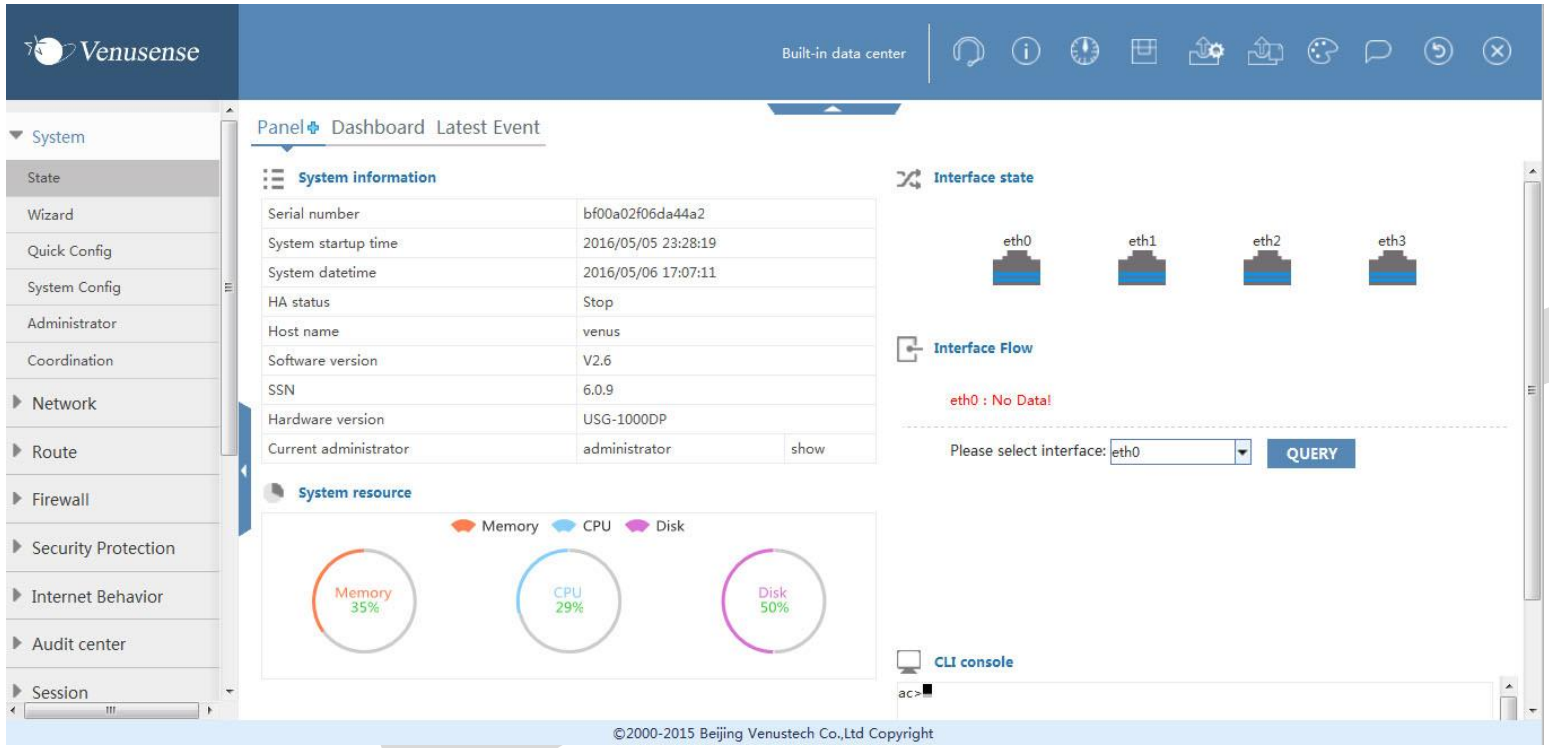
ارتباط امن
Ertebate Amn

به ارتباط امن بپیوند

معرفی محصول
Venustech UTM

معرفی Venustech UTM



کارایی بالا

بکارگیری از معماری پردازش Multi-Core و Multi-Thread

موتور پارس کردن ترافیک

طراحی یکپارچه نرم افزار شامل عملکردهای پایه ای امنیتی مانند: Firewall، Anti-Virus، IPS، Content-Filtering، Application Identification، Anti-Spam، IPSEC/SSL VPN و Anti-DDoS

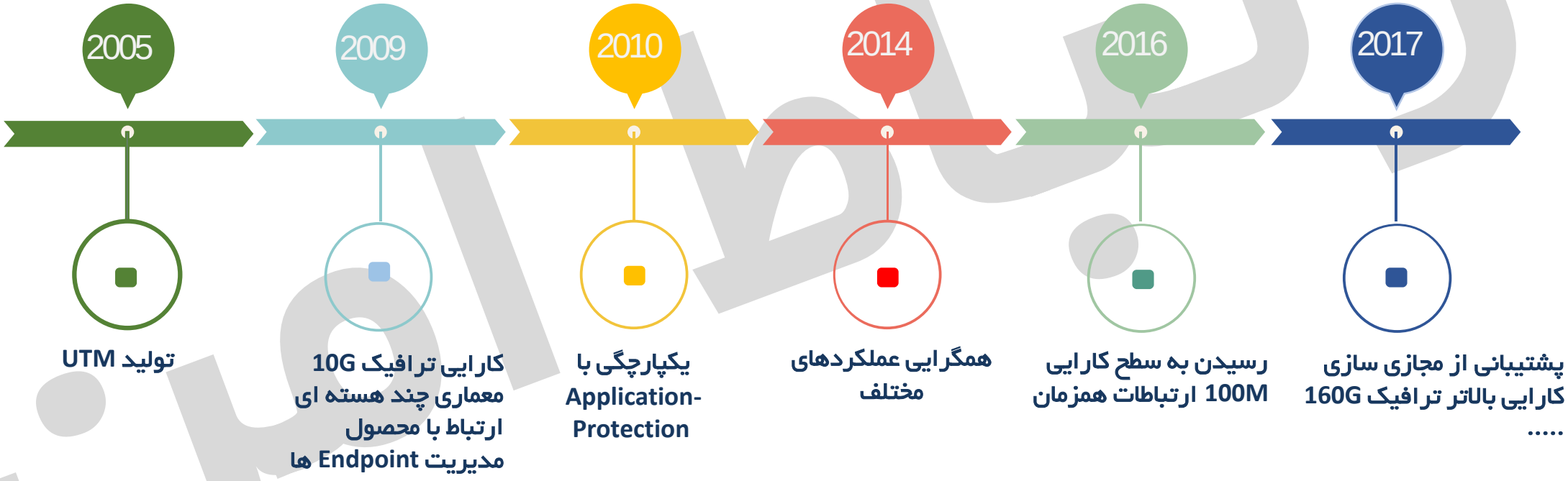
امنیت بر مبنای Cloud

ارائه عملکردهای امنیتی بر مبنای Cloud جهت مقابله با تهدیدات پیچیده جدید

گزارشات

ارائه راهکار پیشرفته مدیریت متمرکز و گزارشات کاربر پسند

نقشه راه Venustech UTM



مدل های Venustech UTM

بیش از ۴۰ مدل (در ۹ سری) جهت پوشش نیاز انواع شبکه ها

ISP

14600GP series

10G high-end device,
40G Throughput,
4Million concurrent connections

16600GP series

10G+ high-end device
80G Throughput

Large enterprise

4000EP series

Quasi 10G device,
10G Throughput,
3.2Million concurrent connections

12600GP series

10G middle-end device,
20G Throughput,

Midsize business

1000DP series

3.5G Throughput,
2Million concurrent connections

2000DP series

5G Throughput,
2.2Million concurrent connections

Small and midsize business

100DP series

For small business and branch office level network,
2G Throughput,
1.2Million concurrent connections

310/610 series

Quasi 1G device,
2G Throughput,
1.8Million concurrent connections

SOHO

70E series

For SOHO level network,
2G Throughput,
1.2Million concurrent connections

Venustech UTM 70E – بالاترین کارایی در بین Desktop UTM ها

سخت افزار

- Intel Bay Trail Platform Quad Core
- Competitive performance
- Wireless module

نرم افزار

- Anti-Virus: Kaspersky engine
- IPS: Powered by Venus ADLAB
- Anti-Spam & URL DB: Cyren Cloud engine

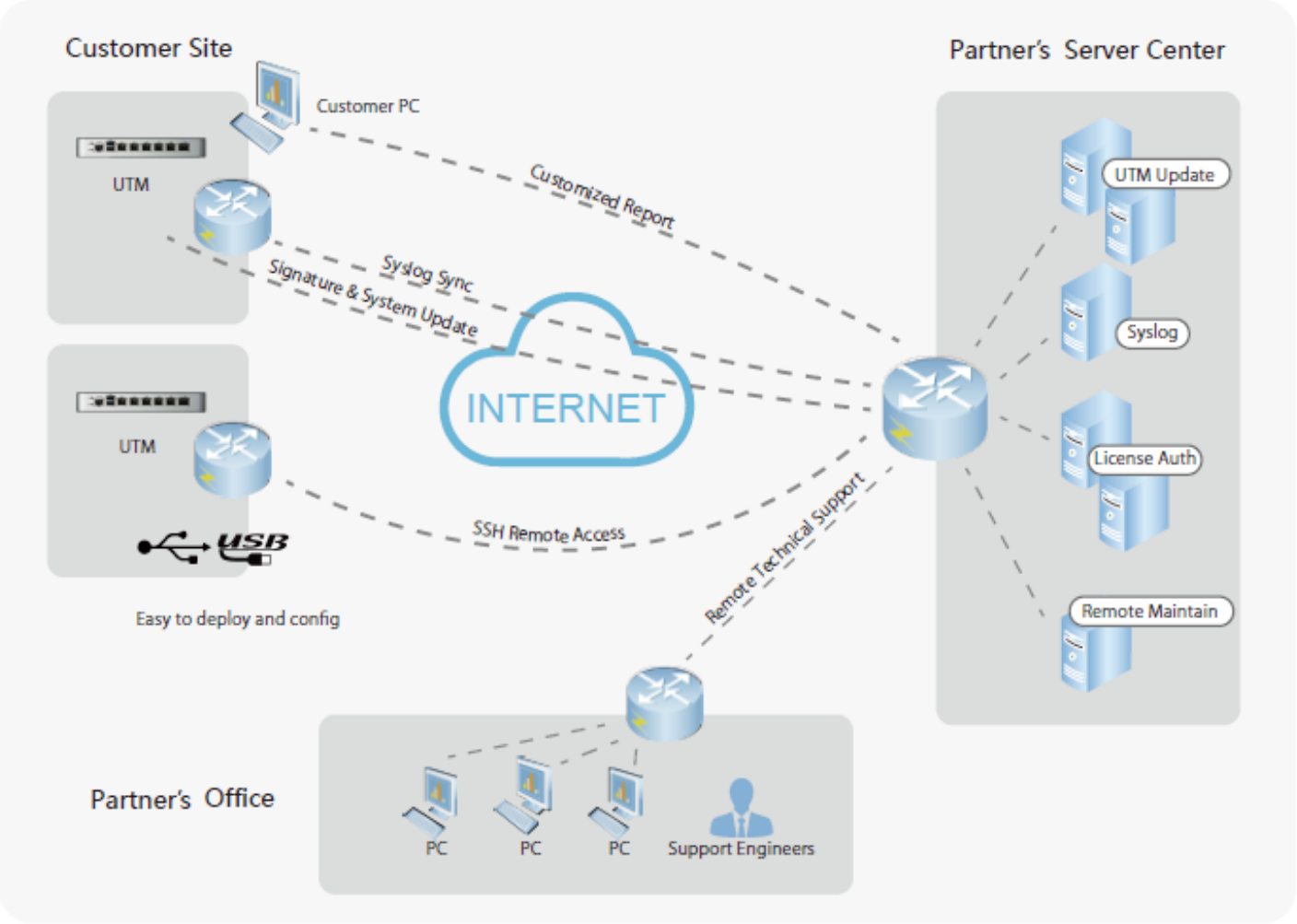
کاربری آسان

- Quick configuration wizard
- Quick configuration via USB driver

شخصی سازی

- Syslog server, Upgrade server, License server, Remote maintenance server.

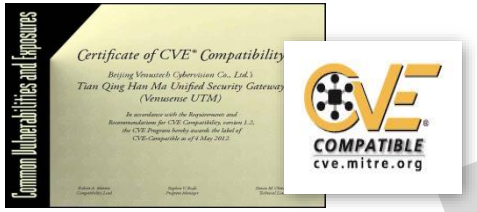
ایجاد ارزش افزوده در مرکز مدیریت



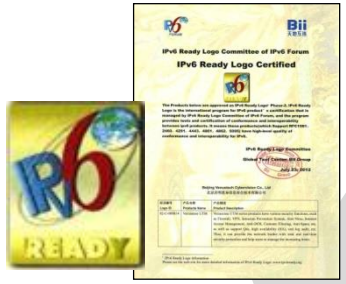
تیم محصول Venustech UTM

گواهینامه ها

- دارای بیشترین گواهینامه های سطح بالا و افتخارات در چین
- دارای گواهینامه های بین المللی



- CVE Compatibility



- IPV6 READY

- Industry Member of Cloud Security Alliance

- Microsoft MAPP Partner

- CE Compatibility

- RoHS Compatibility

- VCCI Compatibility

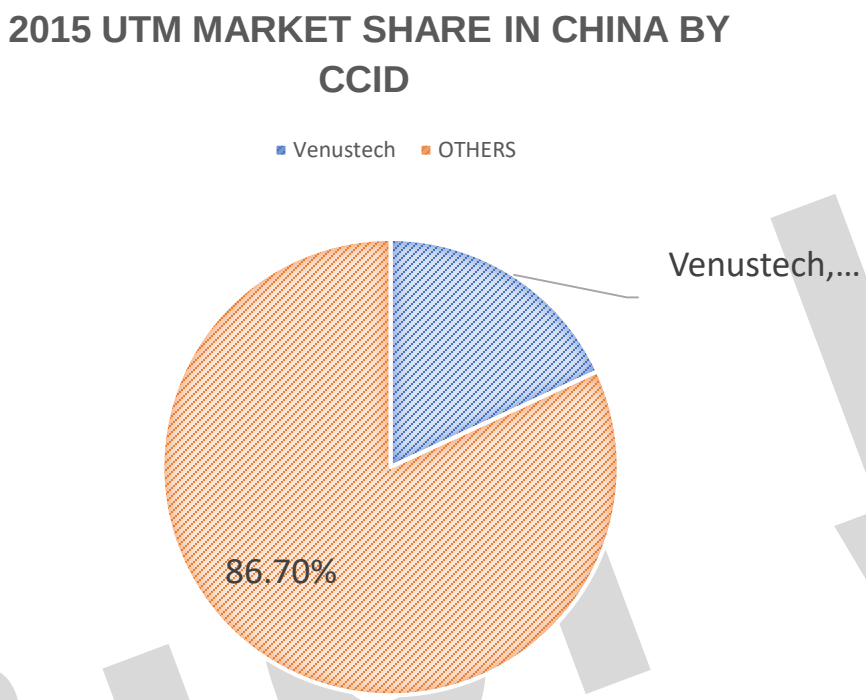
EAL 3+

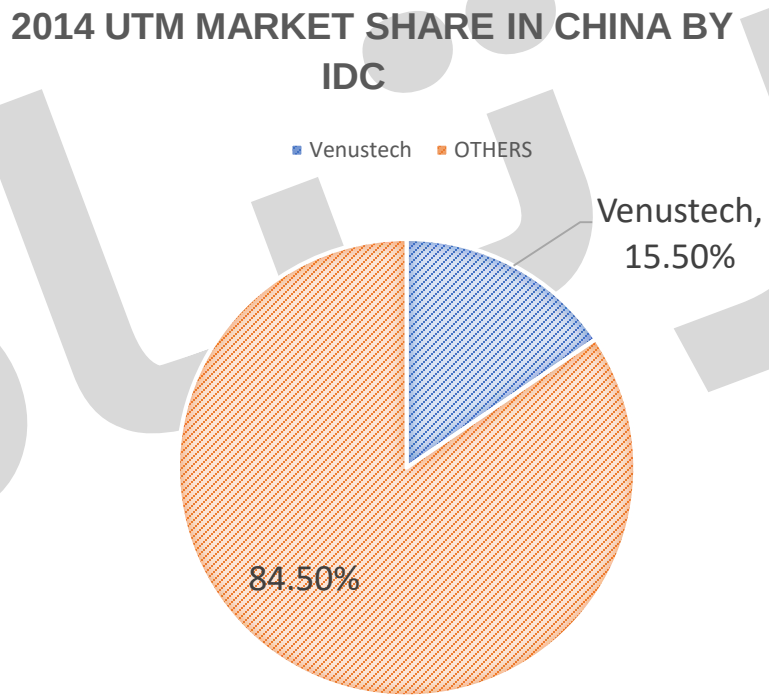
- Security Evaluation

- Patented technology for UTM data processing (Patent No.: 201010270457.6)
- Patented technology for network virus detection (Patent No.: 00810102849.4)
- Patented technology for P2P application identification (Patent No.: 20081022623)0.4)
- Patented technology for virus and intrusion detection (Patent No.: 200610112692.4)

……

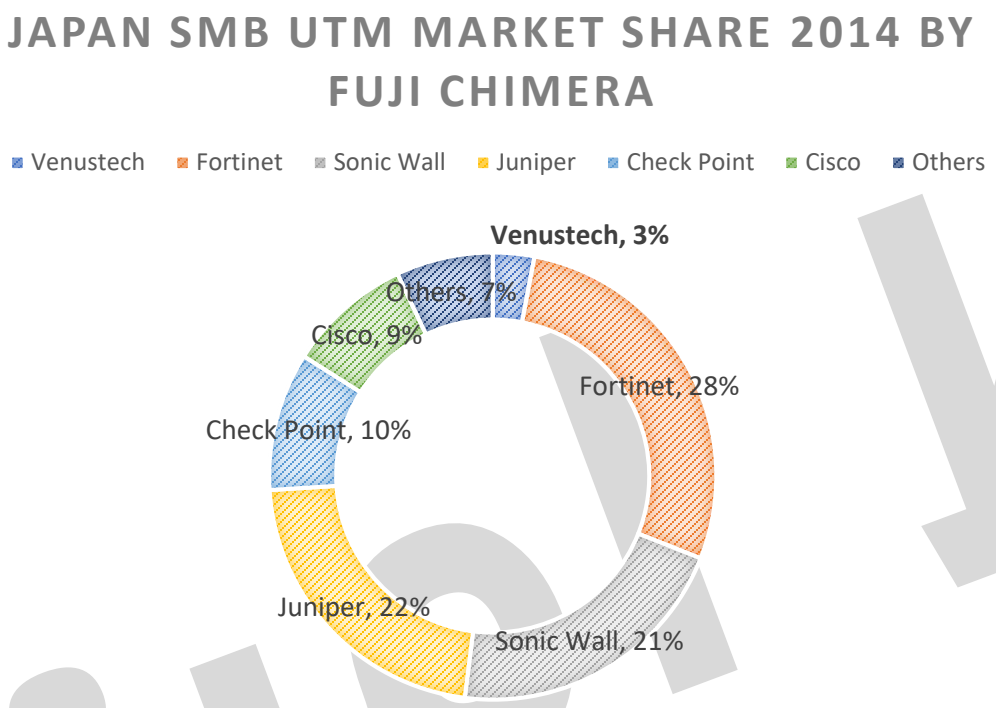
درآمد و سهم از بازار داخلی

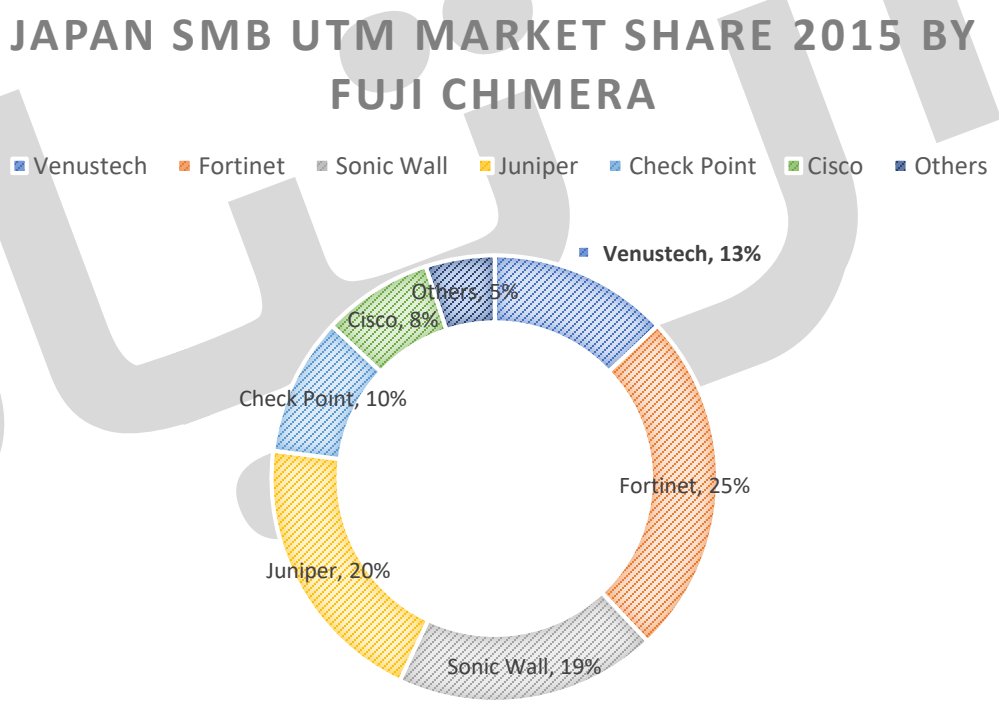




- تا سال ۲۰۱۶ Venustech UTM برای ۶ امین سال متوالی صدر نشین بازار داخلی بوده است.
- فروش در سال ۲۰۱۴: فروش $48.43 Million
- فروش در سال ۲۰۱۵: $62.92 Million
- مجموع فروش UTM و NGFW در سال ۲۰۱۶: $90 Million

سهم بازار از SMB Japan





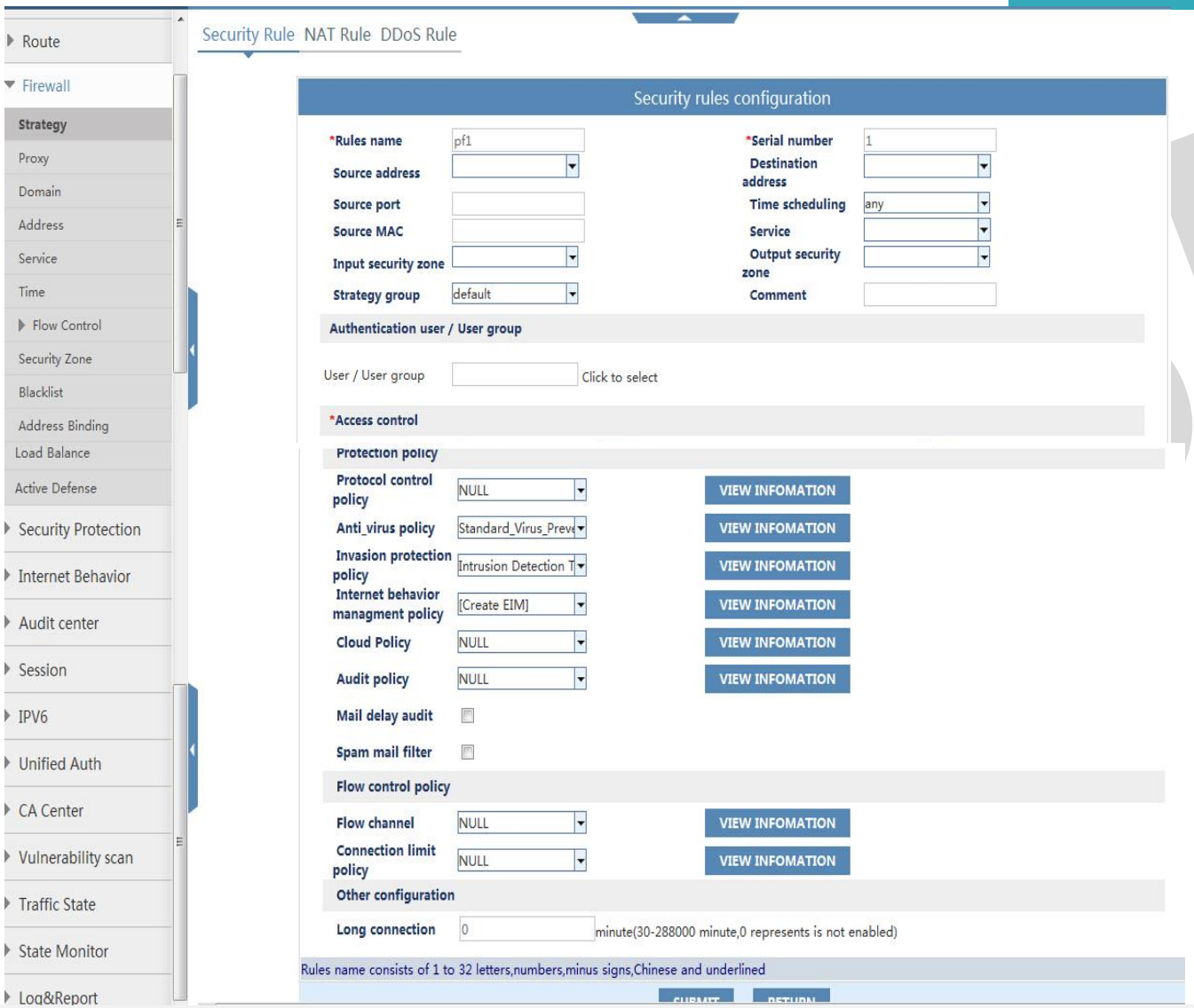
۱۳% از سهم بازار UTM در شرکتهای SMB ژاپنی متعلق به Venustech می باشد. (سال ۲۰۱۵)
جزء ۴ محصول برتر این بازار در سال ۲۰۱۵ است.
جزء ۳ محصول برتر این بازار در سال ۲۰۱۶ است.

تنظیمات مجتمع: امنیت یکپارچه و سیاست های محافظت

Integrated security/protection and traffic control policy:

- All security and protection configurations (such as those for virus defense, intrusion prevention, behavior management and web filtering) are implemented in one unified protection policy.

- User-based application identification and traffic control are implemented based on comprehensive data about users, applications, and content.



امکانات

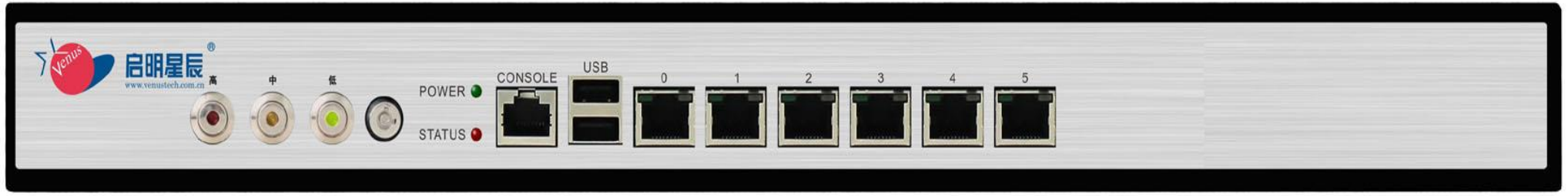
امکان استفاده از تنظیمات از پیش آماده شده

Predefined config switch (for security policy switch)

High - Level3： Absolutely strict security policy. Such as: Standard IPS(Log, Drop, Reset); AV(Drop, Log, all protocols)

Middle - Level2： Relatively strict security policy. Such as: IPS(Log only); AV(Drop, Log for http only)

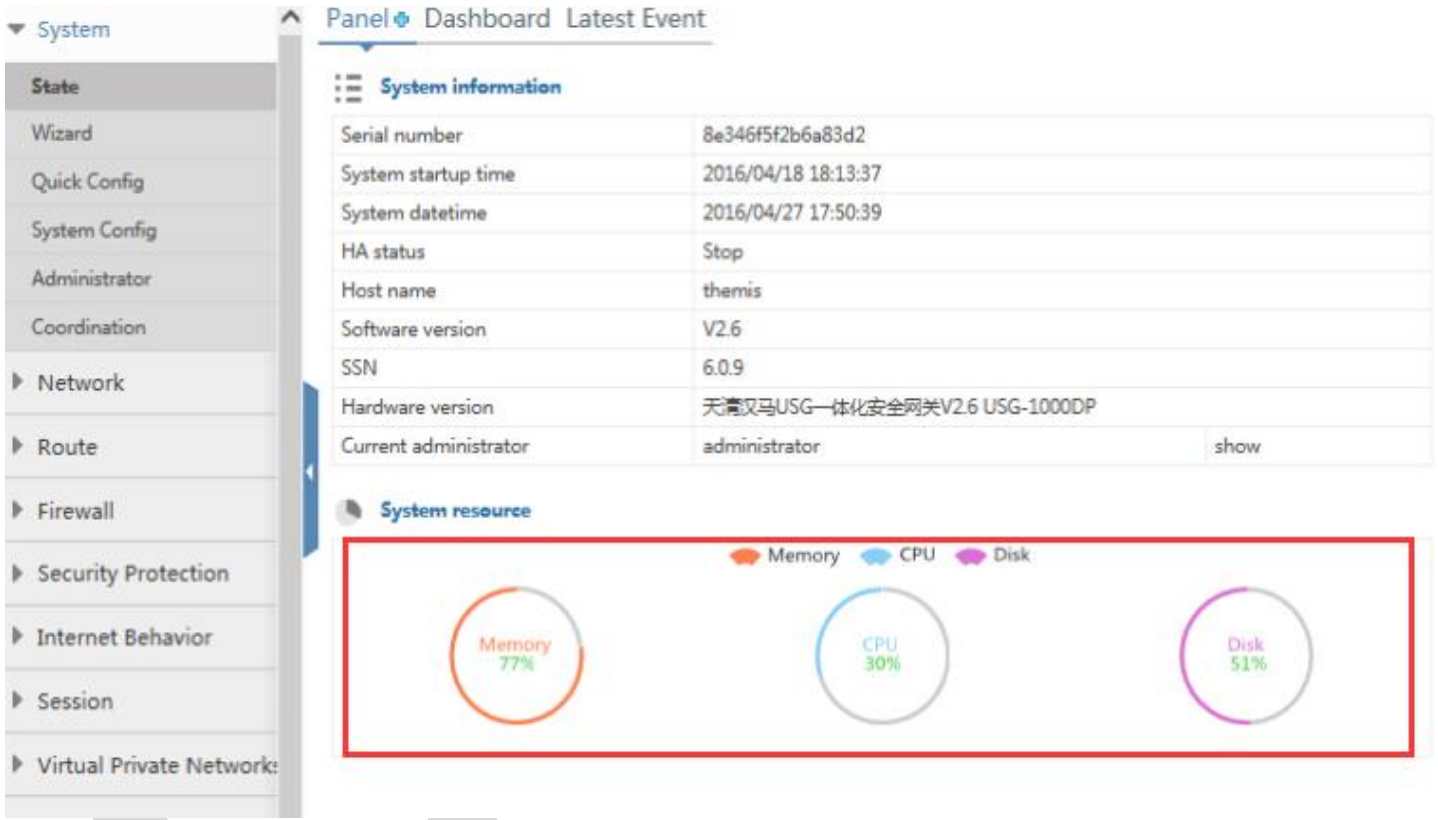
Low - Level1： Less strict security policy. Such as: IPS(Log only); AV(Log only, all protocols)

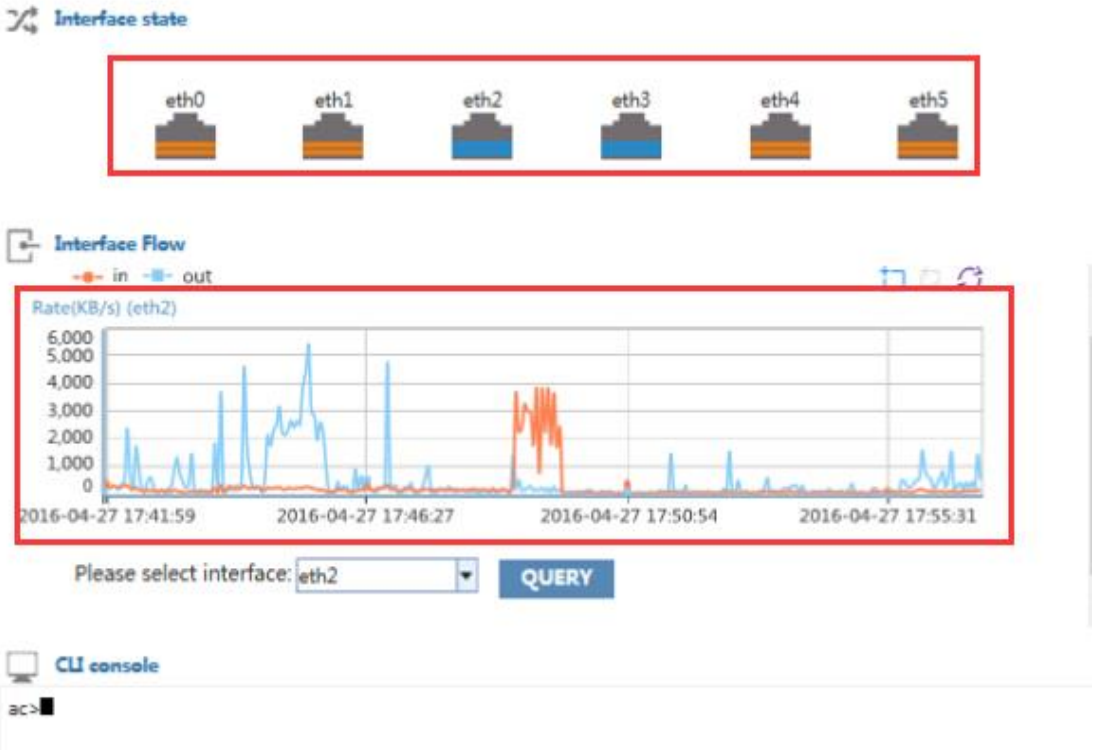


One touch configuration. Easy to use for specific customers.

امکانات

کاربری آسان: نظارت بر منابع و ترافیک





- Display the usage of **Memory, CPU, Disk**.
- Display **the interface status** by colors.
- Display **the real-time traffic flow** for each interface.

امکانات

توانایی های پیش گیری از تهدیدات:
تشخیص ویروس

Local Engine

Kaspersky Engine

Virus Protection Strategy | File Filter | Isolation | Virus Database | Service Port | AV Information

Virus Library

Version 1.3.0.3.405

Regular virus library(Fast Scan)

Number of Contained Features

Description

Standard engine

Enhanced engine

Local engine

Kaspersky engine

Dual-engine mode

Expanded Virus Library(Full Scan)

Number of Contained Features 8351503

Description This library includes the virus emerged in recent years. It is suitable for the high security network.

APPLY

Virus Isolation Settings

Virus File Isolation(Only the Full anti-virus effective)

Isolate File To USB

Virus isolation

Isolate Virus Host(Only the Fast anti-virus effective)

Isolated Virus Sender To Blacklist

Host blacklist

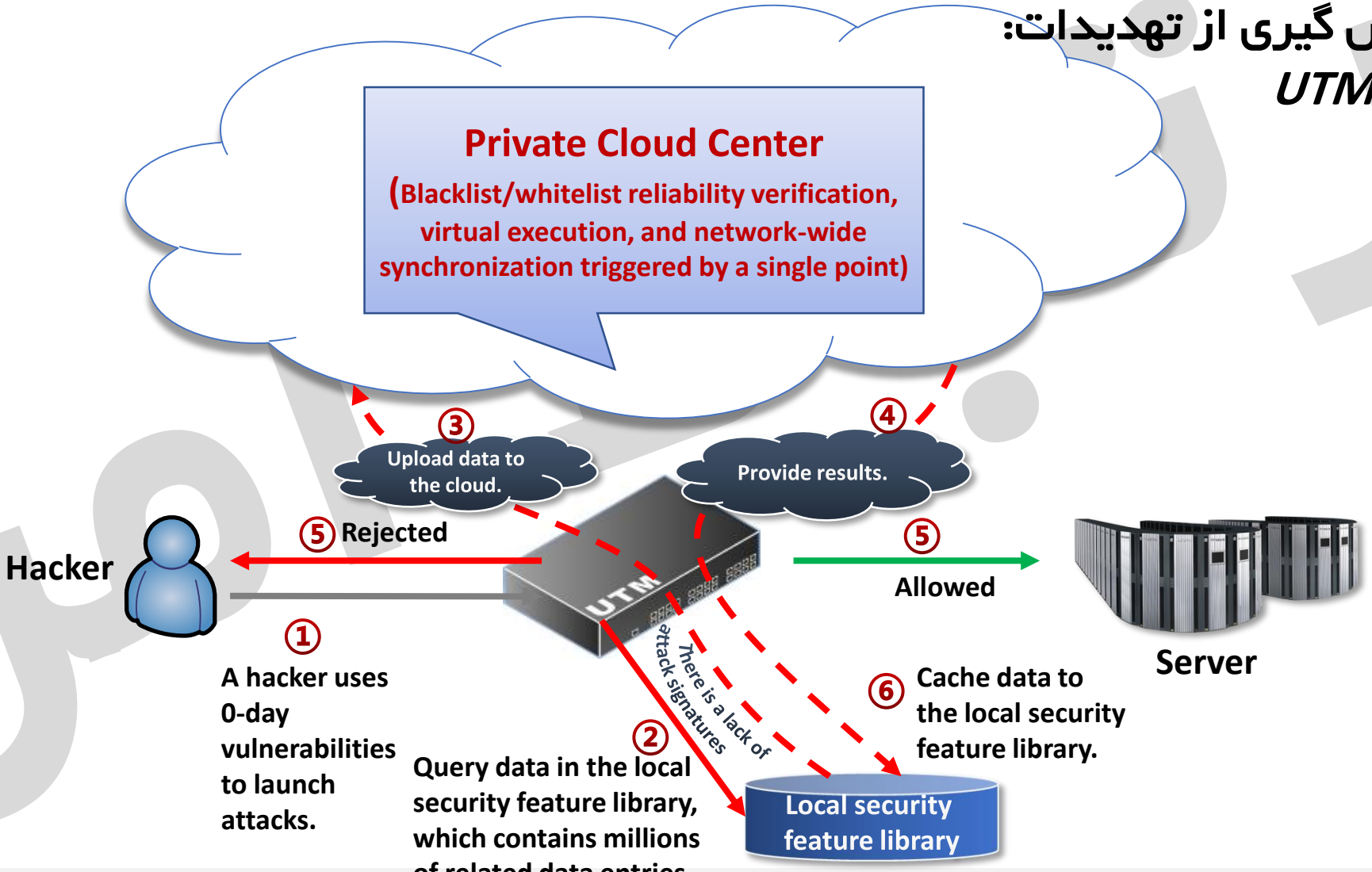
HTTP	FTP	POP3	SMTP
☐	☐	☐	☐

Isolation Time 10 minutes(0 is permanent)

APPLY

امکانات

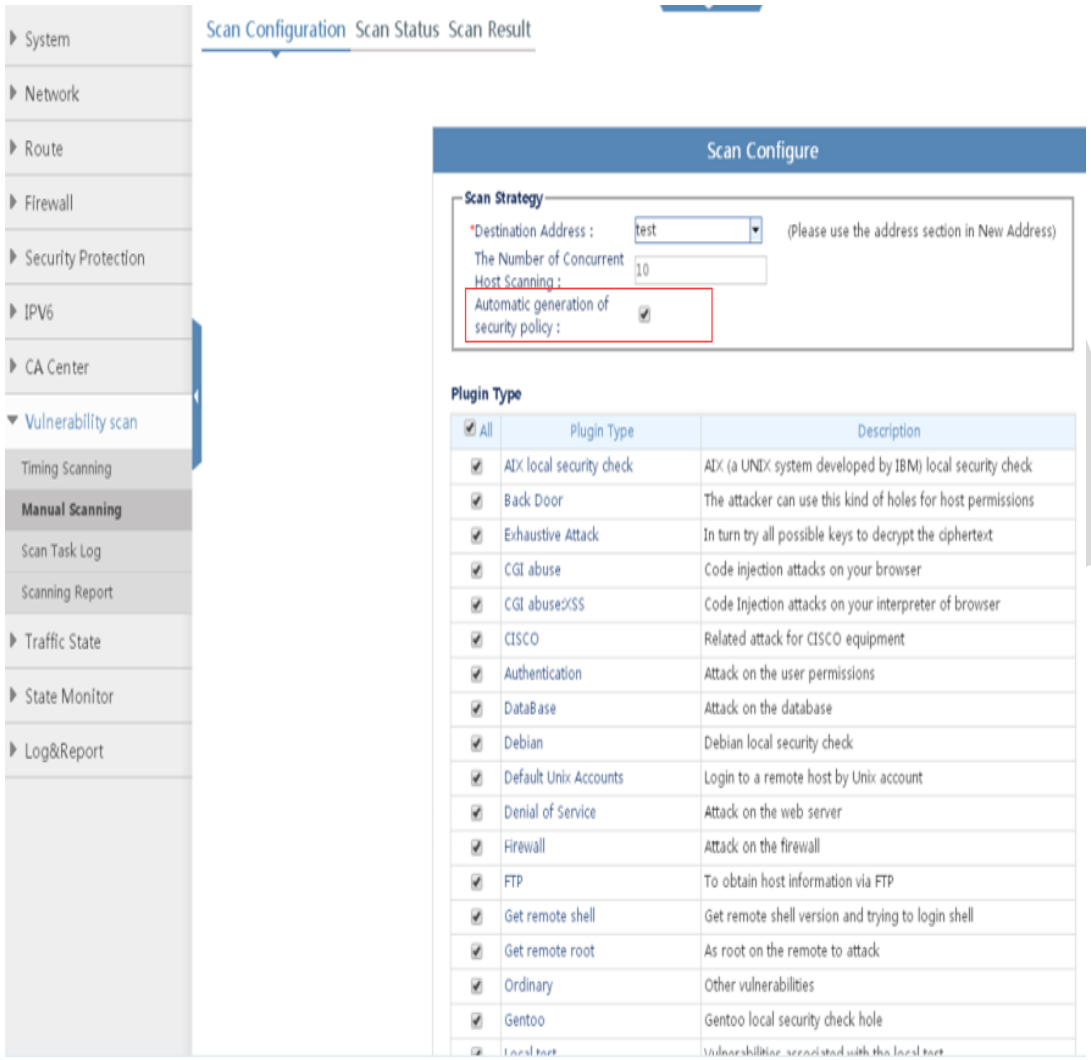
توانایی های پیش گیری از تهدیدات:
UTM+APT solution

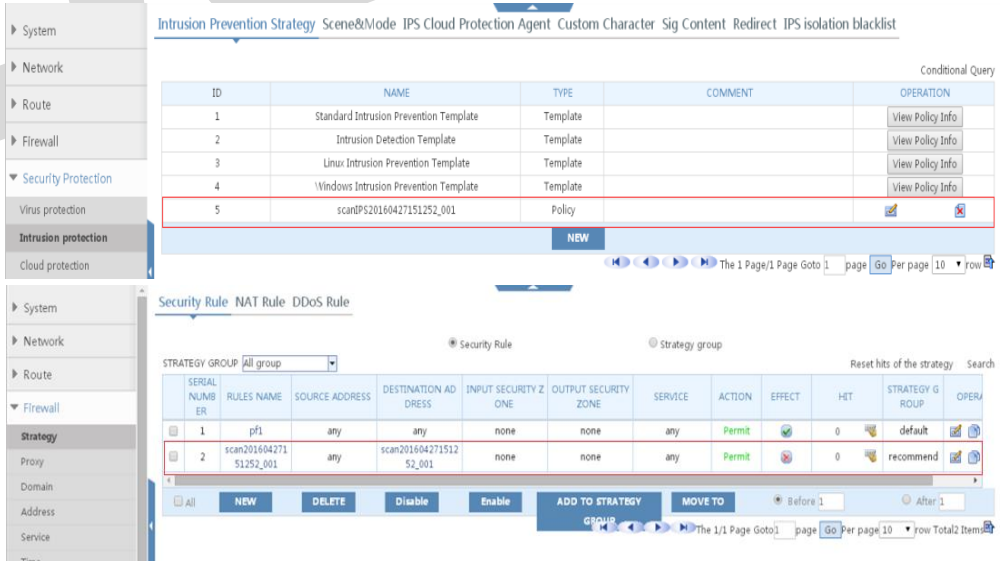


امکانات

توانایی های پیش گیری از تهدیدات:
ایجاد خودکار سیاست های IPS

Vulnerability detection for specified target, intelligently generate the IPS template and prevention policy based on detection result





امکانات

توانایی های پیش گیری از تهدیدات:

IPS blacklist linkage

System
Network
Route
Firewall
Security Protection
Virus protection
Intrusion protection
Anti-spam

Intrusion Prevention Strategy | Scene&Mode | IPS Cloud Protection Agent | Custom Character | Sig Content | Redirect | IPS isolation blacklist

Log View | Security Rule

Log Server Settings | Log Type : All logs | Log Priority : All | Please enter a keyword | SEARCH

DATE	MESSAGE	LEVEL	TYPE	DEVICE NAME	ACTION	SOURCE ADDRESS	DESTINATION ADDRESS	DETAIL
2016/05/05 16:32:56	Show IPS isolation blacklist list page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:52	Show IPS Isolation Blacklist Settings page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:52	Show IPS Isolation Blacklist Settings page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:49	eth2 link up	Note	Device state log	themis	show	----	----	Click to view...
2016/05/05 16:32:49	Show ipspolicy list page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:47	eth2 link down	Note	Device state log	themis	show	----	----	Click to view...
2016/05/05 16:32:31	Show Log Show page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:25	Show Log Show page	Information	Device management log	themis	show	10.16.1.2	----	Click to view...
2016/05/05 16:32:22	Detect attackhttp_host; type:UserDefine	Warning	IPS log	themis	drop	10.16.2.1	220.181.111.188	Click to view...
2016/05/05 16:32:22	add blacklist ip=10.16.2.1	Note	Device management log	themis	add	----	----	Click to view...

Address
Service
Time
Blacklist

equent Access

Improve the processing efficiency of IPS

Office network

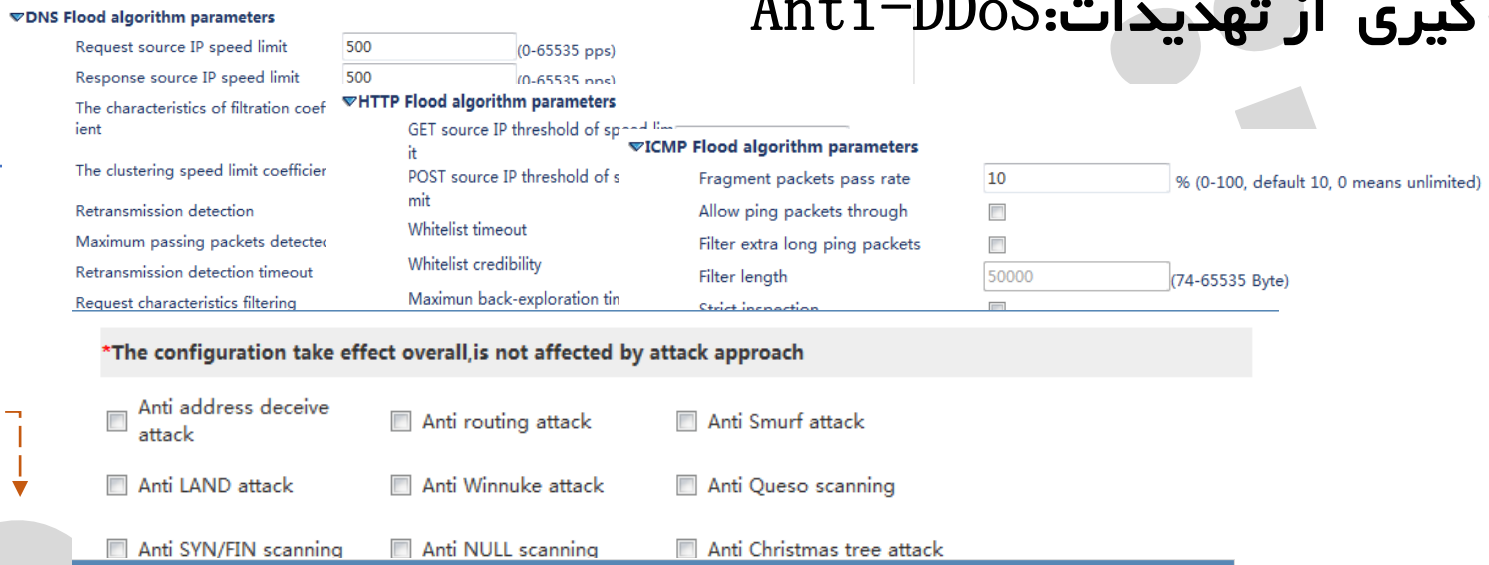
امکانات

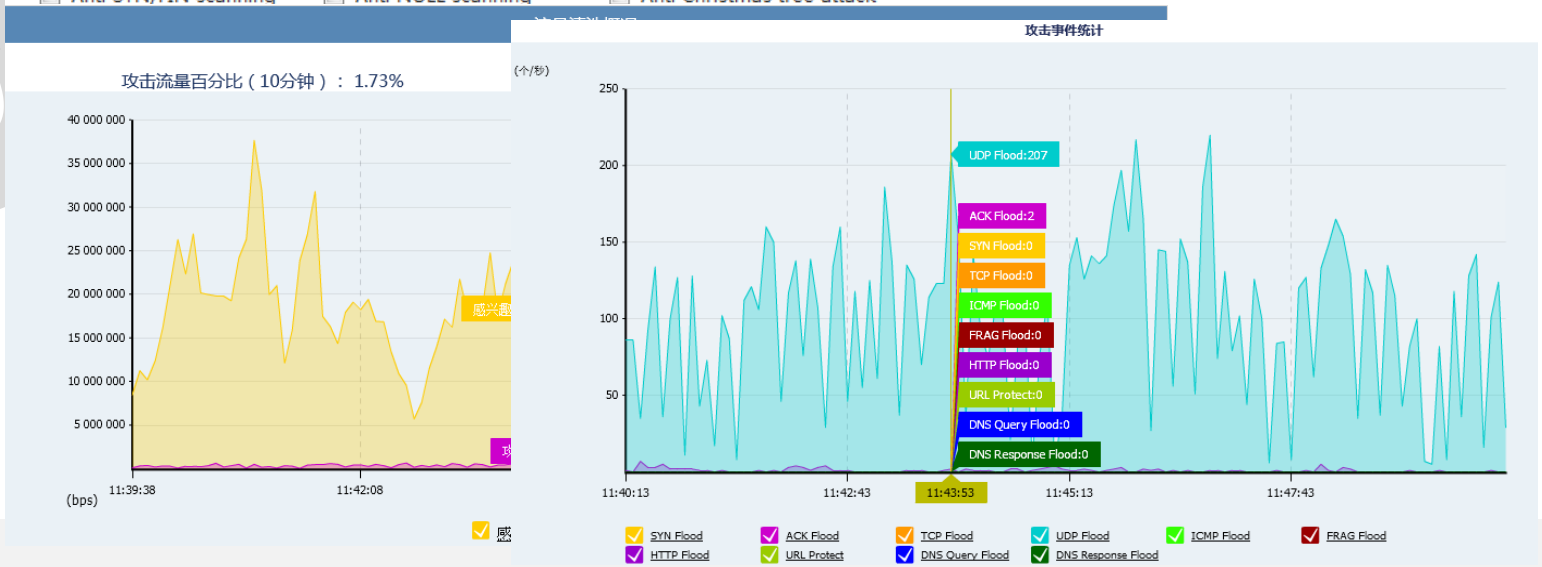
توانایی های پیش گیری از تهدیدات:Anti-DDoS

Fine grained detection algorithm

Global configuration

Attack traffic statistic





امکانات

توانایی های پیش گیری از تهدیدات:*URL self-learning*

URL Policy | Custom URL | URL Config | URL List | Intelligent Learning | Learning Resu

ID	NAME	KEYWORD
1	Tourism and Travel	
2	Cosmetology	
3	Web Proxy	
4	Newspapers and Magazines	
5	Portal Site	google,
6	Recruitment	linkedin,51job
7	Finance and Securities	
8	Adult Site	
9	Software	
10	Children	

URL Config | URL List | Intelligent Learning | Learning Result

URL config

URL recognition

Enable ☑

Intelligent recognition feature lib cache: 30 (Range:11-100M)

Server ip:

Server port: 0

0

Enable ☐

Enable ☐

IP address access is prohibited

Enable ☐

SUBMIT

User self-service-extendable URL library

Office network

ارتباط امن
Ertebate Amn

امکانات

Content visibility: Webmail, Forum, Twitter, Uploading content, Email content, Webpage content

Add Audit Policy

*Name (Name consists of 1 to 32 letters,numbers,minus signs,Chinese and underlined)
Comment (0-255 characters)

HTTP out
- Web mail content
  - Web appendix content
- Web text content
- Web bbs content
- Microblog content
  - Microblog appendix

HTTP up/download
- PUT file filename and content
- GET file filename and content

HTTP access website
- Access URL
  - All URL
    - Appoint URL
- Web content
  - Only audit web title
  - Audit web title and content
    - All URL
    - Appoint URL
- By keyword set of audit

FTP up/download
- PUT file filename and content
- GET file filename and content

Mail
- Send mail content(SMTP)
- Receive mail content(POP3)

Group Name:/root | Have Subgroups:Yes | Statistical Time:Custom | Date:2016-04-27 - 2016-04

Risk Intelligence Reports
Contrast Report
Statistics
Log Query
- Online Behavior
  - All Online Behaviors
  - Visit Website
  - Mail Send/Receive
  - IM Chat
  - Account Audit
  - Forum Posting
  - Outgoing File
  - Outgoing Information(HTTP)
  - File Upload(FTP)
- Online Traffic
- Internet Time
- Firewall Log

Trend
System Managerment

Query Results of All Online Behavior

	User Name	Group Name	Host IP	Destin
11	chenkn	/root/test	192.168.84.128	220.1
12	chenkn	/root/test	192.168.84.128	220.1
13	baibing	/root/test2	192.168.84.50	192.1
14	chenkn	/root/test	192.168.84.128	121.1
15	chenkn	/root/test	192.168.84.128	121.1
16	chenkn	/root/test	192.168.84.128	121.1
17	chenkn	/root/test	192.168.84.128	220.1
18	chenkn	/root/test	192.168.84.128	121.1
19	chenkn	/root/test	192.168.84.128	121.1
20	chenkn	/root/test	192.168.84.128	121.1

10 Page 2 Go of 31432

©2000-2015 Beijin

Statistical Condition | Collection | Export Log

| Time:00:00:00 - 23:59:59 | Email Type:All Types

Order Date And Time

	Email Header	Abstract	Email From	Email To	Specific Application	User Name	In The Group	Email State	Time
31	[3.6.0.9升级包定制版本	下列问题已经提交 ====	Mantis Bug Tracker	liurr@leadsec.com.cn	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
32	[3.6.0.9升级包定制版本	下列问题已经提交 ====	Mantis Bug Tracker	liurr@leadsec.com.cn	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
33	截图	_____	黄涛	"=liurr="	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
34	[3.6.0.9升级包定制版本	下列问题已经提交 ====	Mantis Bug Tracker	liurr@leadsec.com.cn	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
35	回复: 最晚下班前反馈—	姓名 测试用例输出数据	"wulb@leadsec.com.cn	liurr	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
36	11000J测试进展反馈	已完成：3类口的UDP吞	"weigd@leadsec.com.c	董楠楠	Receive Email	192.168.84.56	/root/test	Send or Receive Succe	2016-04-27 15:38:23
37	【问题反馈】海外版本临	Hi，二位： 根据提交单，	xieqi@leadsec.com.cn	gaopeng@leadsec.con	Send Email	xieqi	/root/test	Send or Receive Succe	2016-04-27 15:37:25
38	转发:【借用申请单审批	发件人: 占芬芬（集团外	张其华	=杨召辉=	Receive Email	192.168.84.122	/root/test	Send or Receive Succe	2016-04-27 15:35:37
39	11000J测试进展反馈	已完成：3类口的UDP吞	weigd@leadsec.com.cn	dongnn@leadsec.com.	Send Email	weigd	/root/test2/test3	Send or Receive Succe	2016-04-27 15:32:14
40	回复: 最晚下班前反馈—	姓名 测试用例输出数据	wulb@leadsec.com.cn	liurr@leadsec.com.cn	Send Email	wulb	/root/test2	Send or Receive Succe	2016-04-27 15:29:08

10 Page 4 Go of 17 — Displaying 31 to 40 of 166 items

192.168.84.56 — 2016-04-27 15:38:23

Email From: Mantis Bug Tracker <mantis@leads — Email To: liurr@leadsec.com.cn — Download original email

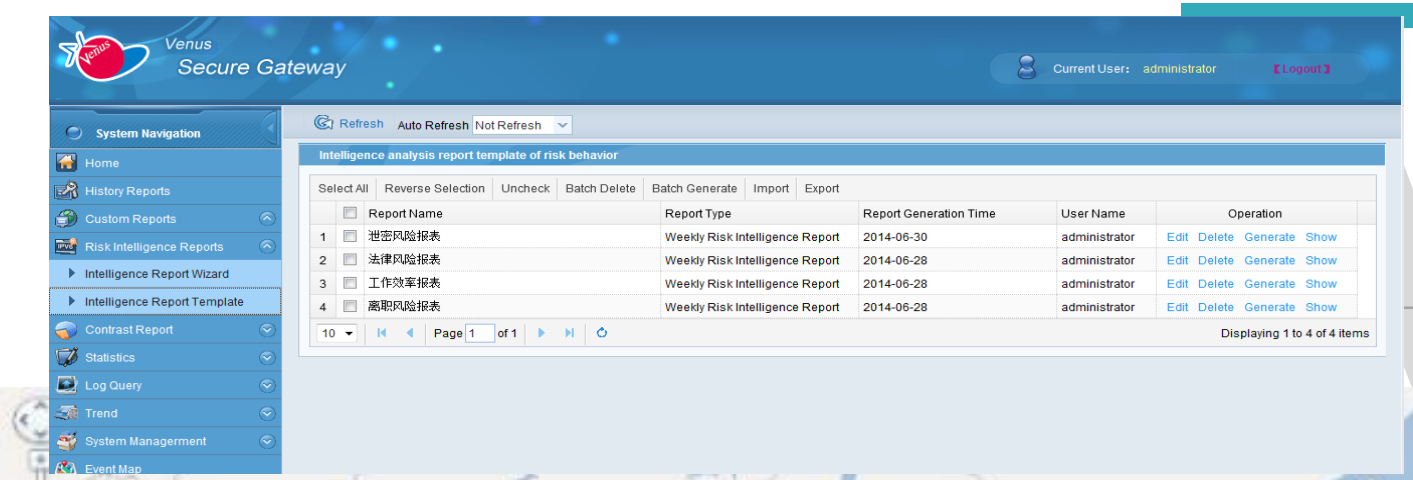
Email Header: [3.6.0.9升级包定制版本测试 0043506]: 【3.6.0.9(43226)UP-g- 05-3.6.0.9-1功能升级包_HA】会话保 护模式的配置同步，应用防护反垃 圾邮件配置两台...

Email Content — Attachment Number: 0

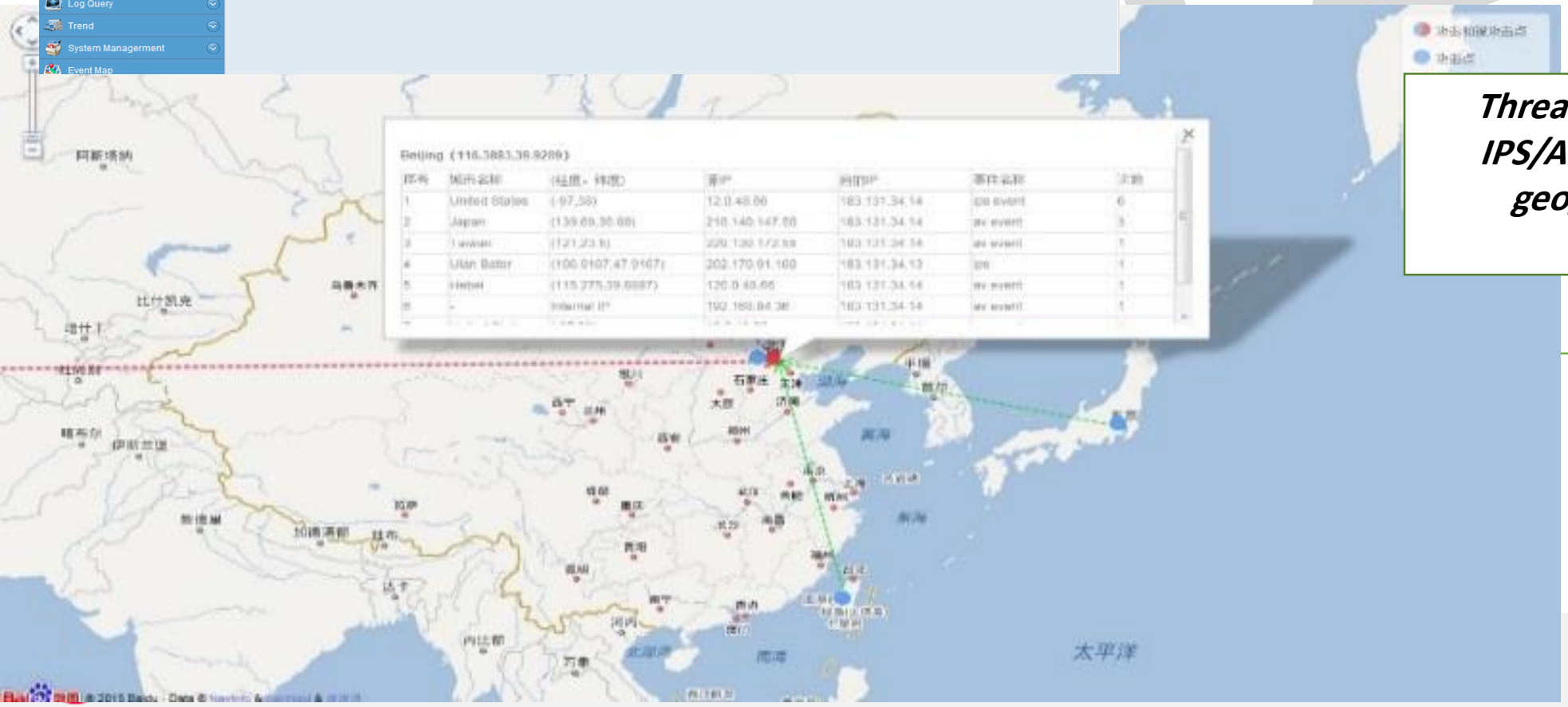
下列问题已经提交 ========== https://192.168.84.247/mantis/view.php?id=43506

Venustech

امکانات

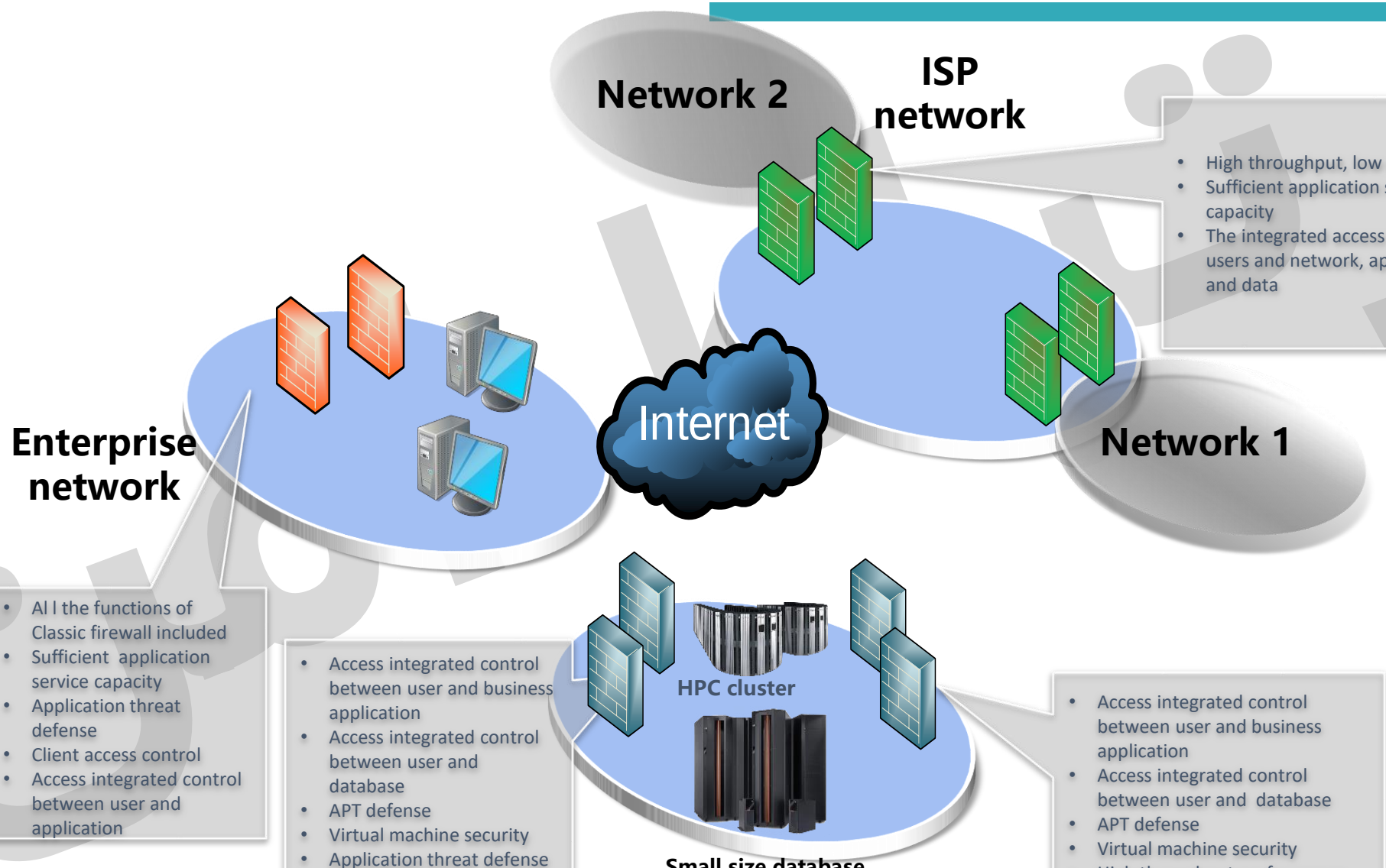


Risk visibility: Data Leakage, resignation analysis and legal risk visibility



Threat visibility: real-time IPS/AV event ranking and geographical incident presentation

سناریوی پیاده سازی UTM



- High throughput, low delay
- Sufficient application support capacity
- The integrated access between users and network, application and data

- Al l the functions of Classic firewall included
- Sufficient application service capacity
- Application threat defense
- Client access control
- Access integrated control between user and application

- Access integrated control between user and business application
- Access integrated control between user and database
- APT defense
- Virtual machine security
- Application threat defense

- Access integrated control between user and business application
- Access integrated control between user and database
- APT defense
- Virtual machine security
- High throughput performance requirement

Enterprise deployment

Datacenter deployment

ISP deployment

مورد کاربرد ۱ : راه حل امنیتی شبکه خصوصی دولت

3-stage security network constructing for the provincial audit bureau(HQ, Branch, Sub-branch)

Target

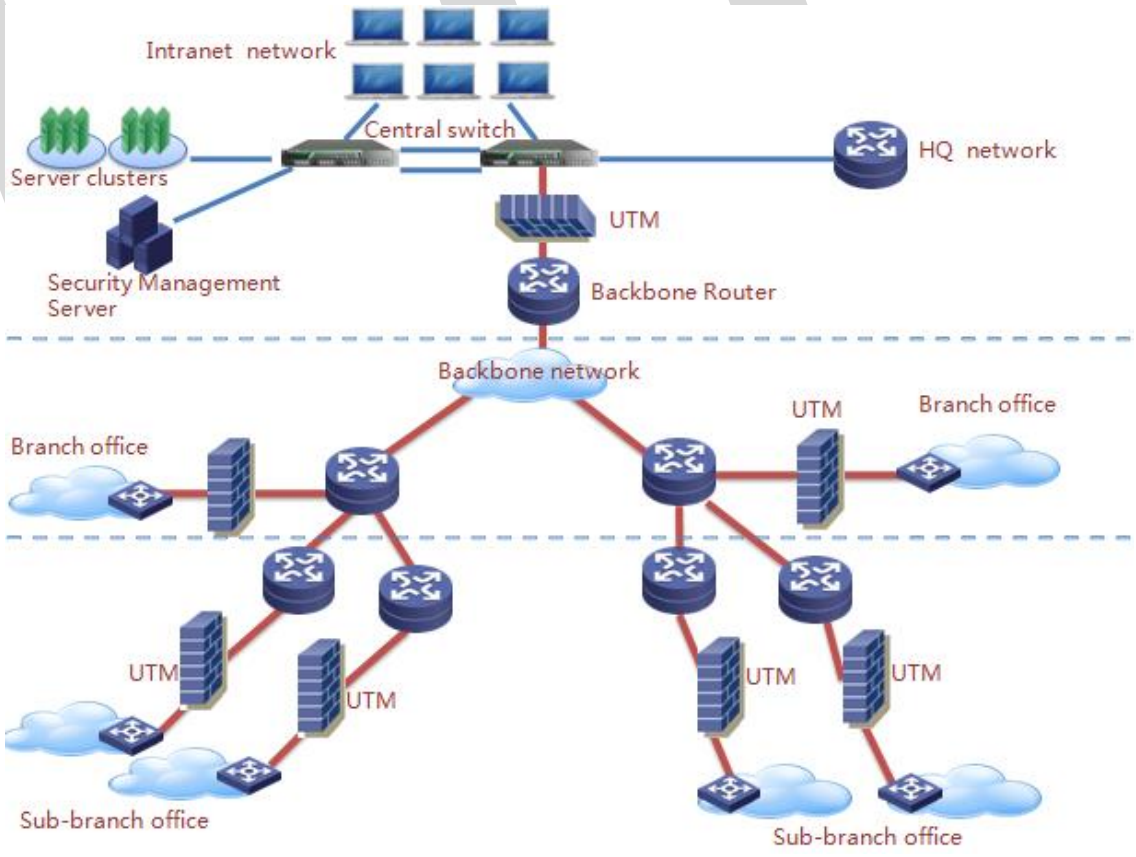
Considered the business ,geography location and administrative structure , the network is separated to several secure domain. Between the secure domains, the access control, intrusion and illegal access prevention, virus and worm prevention are properly realized.

Scale

The quantity PCs and servers in the business system are more than 3000.

Solution

- Use Venusense UTM to realize the function instead of the traditional Firewall , IPS and internet behavior management products. Deploy the system for the entire province in 3 weeks without any network structure changing and working interrupting.
- The high-end UTM and integrated security management platform is deployed at the provincial Bureau HQ ,in this way ,the whole system is easily to management ,audit , analysis and update. ;
- Deploy the Mid-end Venusense UTM at the municipal office of the audit bureau, the UTM supports to configure automatically by pressing only one button even there is no professional technique staff .



مورد کاربرد ۲: راه حل امنیتی سیستم مدیریت کاربران ISP

Network security system modernization project for the accounting system of a provincial ISP

Target

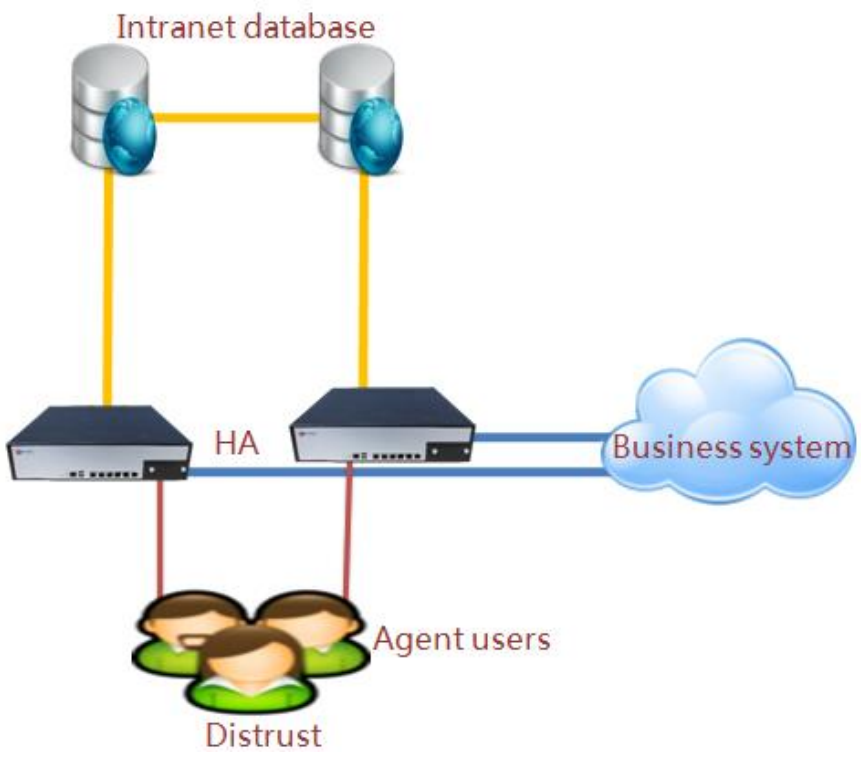
The data center is crucial for the business system of the ISP ,but the client security is uncontrollable because of kinds of virus and worms spreading, therefore, it is vital to solve the secure issue at the client side to guarantee the security of the entire business system.

Scale

The core business system of the ISP is responsible for accounting and service fulfillment ,the client sum is more than10000.

Solution

- Deploy the high-end Venusense UTM (40G throughput) in front of the intranet database and core business system, the front side of the UTM is the agent client which need to access the core business system and the back side is the business server clusters of the ISP which provides the core service ;
- Due to the high availability and persistency requirements of the ISP's business system, deploy 2 UTMs working as HA.



ارتباط امن

Ertebate Amn

Thank you