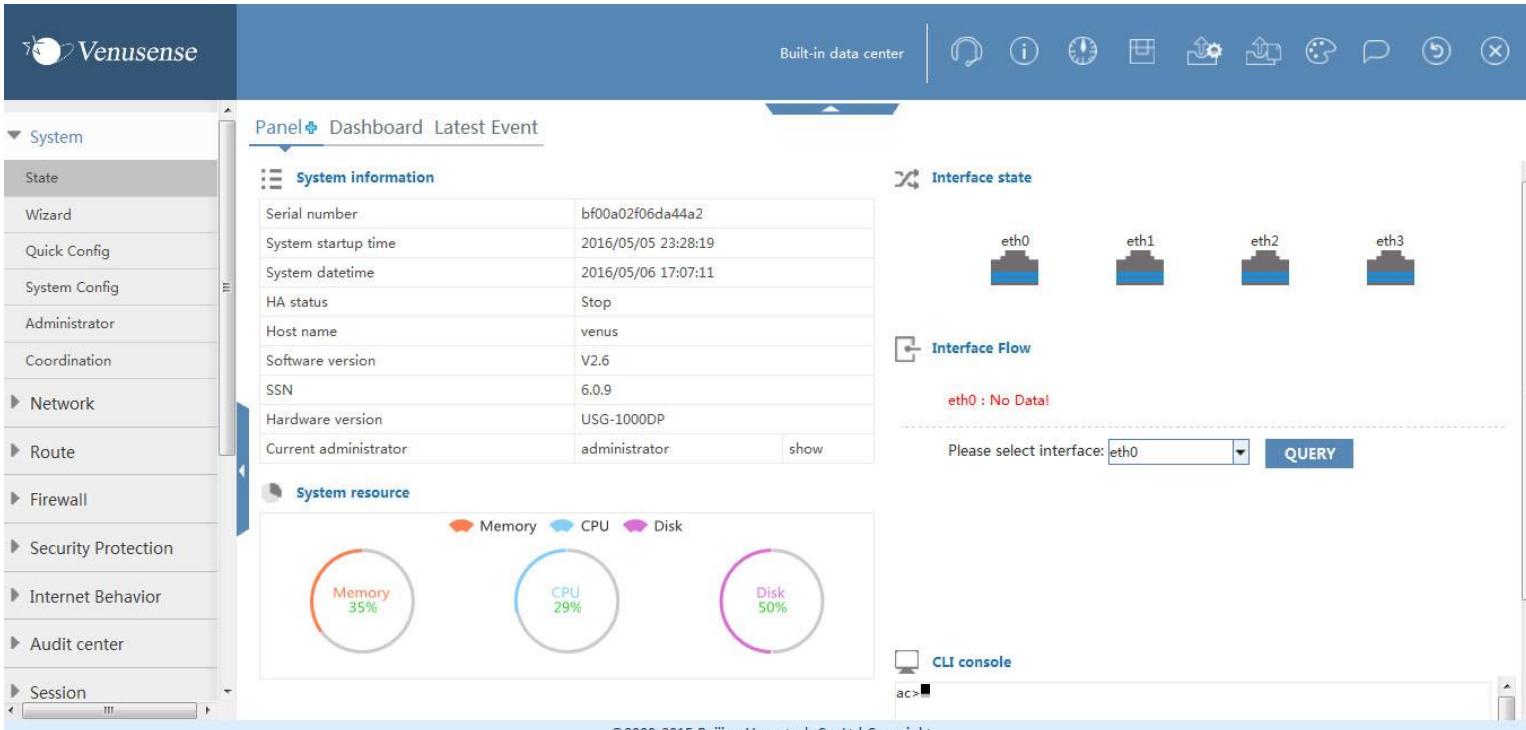




به ارتباط امن پیوند

معرفی محصول Venustech UTM



Venusense

Built-in data center

Panel Dashboard Latest Event

System information

Serial number	bf00a02f06da44a2
System startup time	2016/05/05 23:28:19
System datetime	2016/05/06 17:07:11
HA status	Stop
Host name	venus
Software version	V2.6
SSN	6.0.9
Hardware version	USG-1000DP
Current administrator	administrator
	show

System resource

- Memory: 35%
- CPU: 29%
- Disk: 50%

Interface state

eth0 eth1 eth2 eth3

Interface Flow

eth0 : No Data!

Please select interface:

CLI console

```
ac>
```

©2000-2015 Beijing Venustech Co.,Ltd Copyright



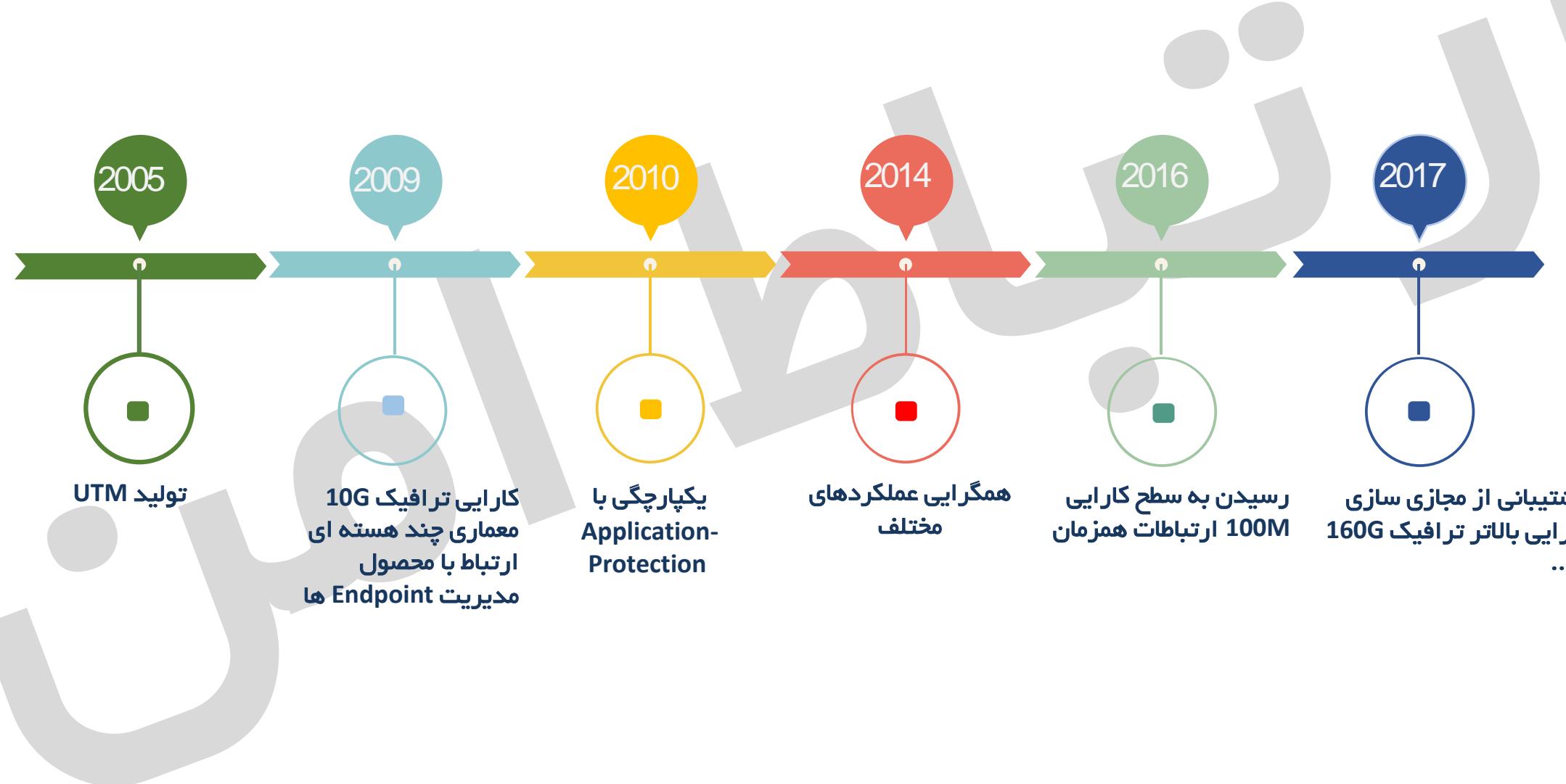
کارایی بالا
بکارگیری از معماری پردازش Multi-Core و Multi-Thread
موتور پارس کردن ترافیک
طراحی یکپارچه نرم افزار شامل عملکردهای پایه ای امنیتی مانند: Anti-Virus، Firewall، Application، Content-Filtering، IPS، IPSEC/SSL، Anti-Spam، Identification، Anti-DDoS و VPN



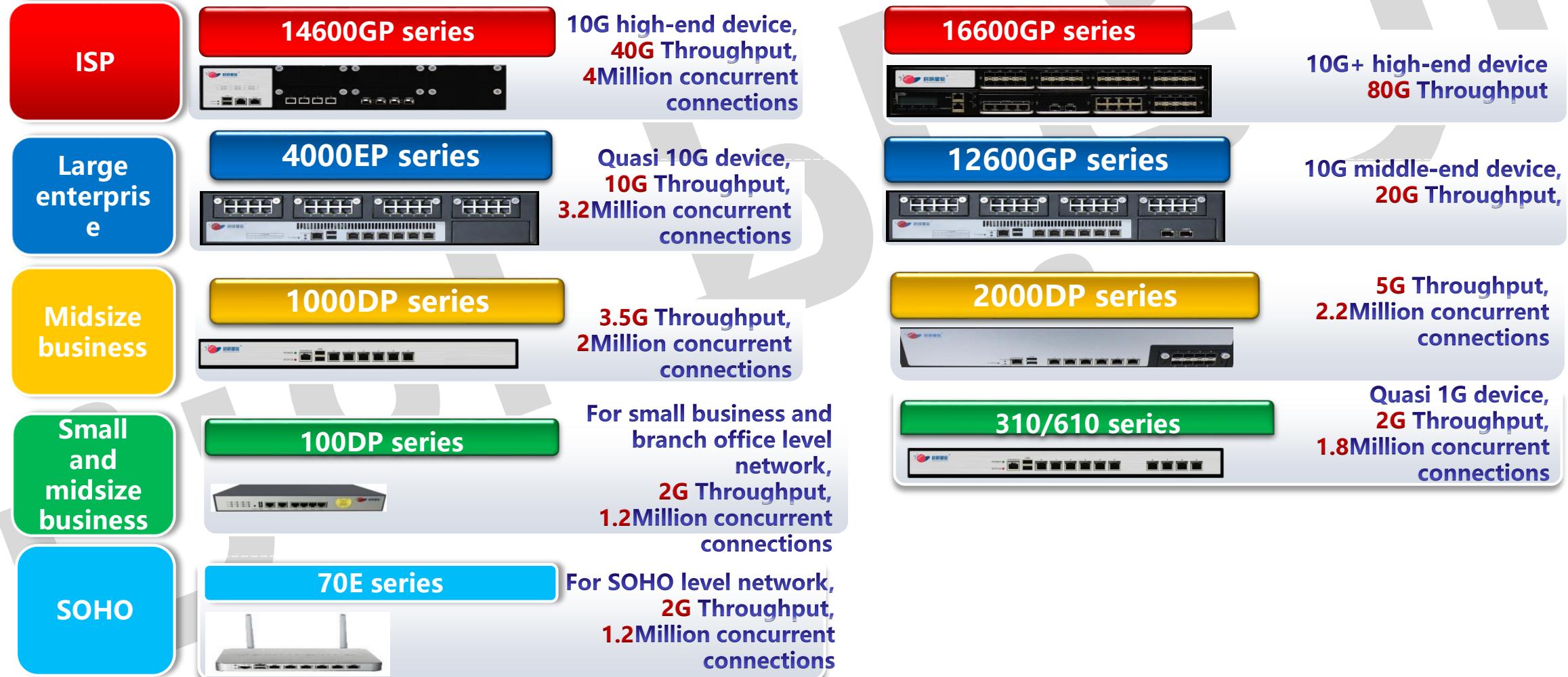
امنیت بر مبنای Cloud
ارائه عملکردهای امنیتی بر مبنای Cloud جهت مقابله با تهدیدات
پیچیده جدید



گزارشات
ارائه راهکار پیشرفته مدیریت مرکزی و
گزارشات کاربر پسند



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

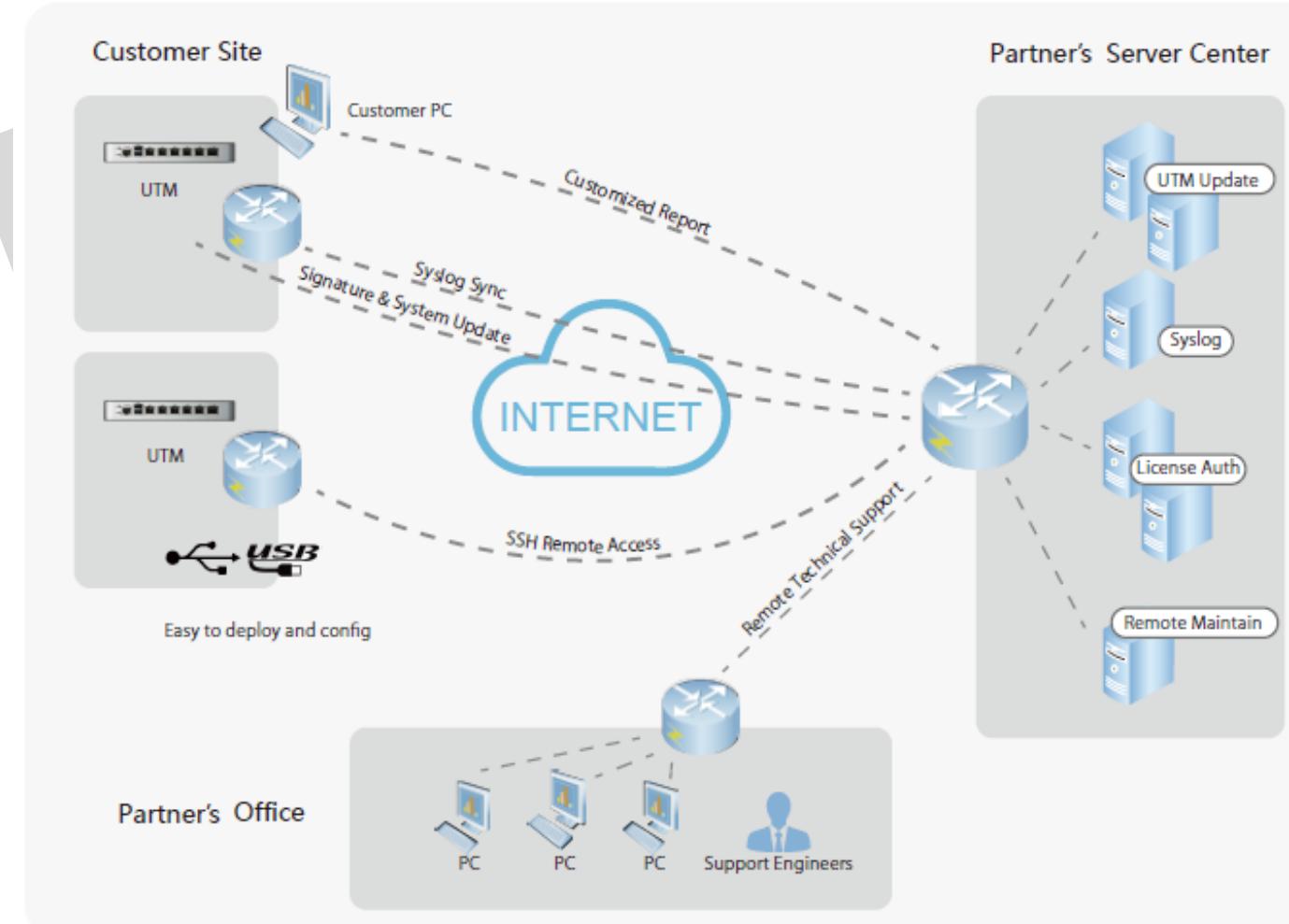
کاربری آسان

- 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



UTM Products Team 210 staffs

R&D

120 staff

Planning &

design

12 staffs

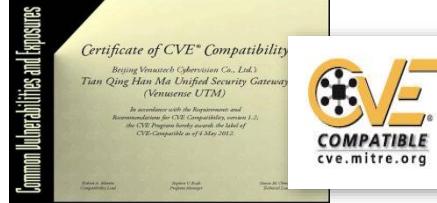
QA

70 staffs

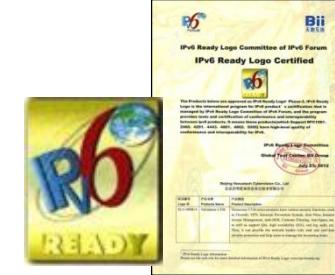
Tech specialists

8 staffs

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



- CVE Compatibility



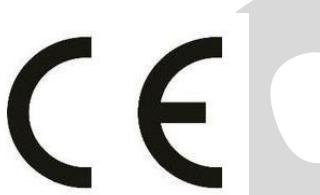
- IPV6 READY



- Industry Member of Cloud Security Alliance



- Microsoft MAPP Partner



- CE Compatibility

- 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)

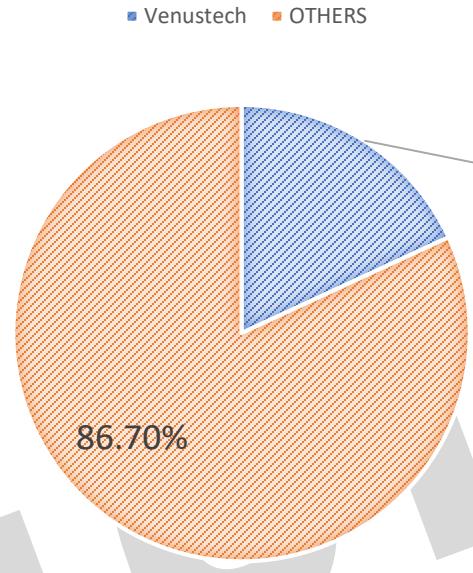


- RoHS Compatibility
- VCCI Compatibility

EAL 3+

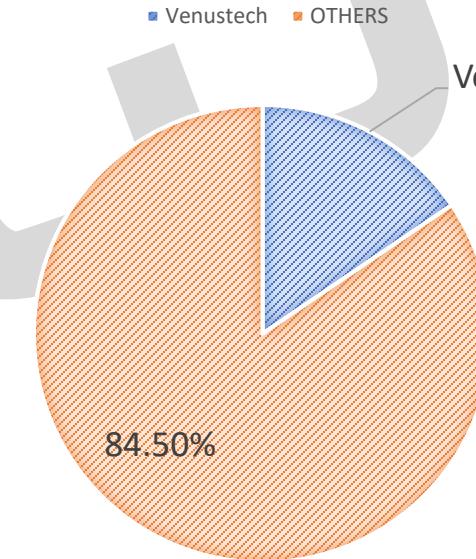
- Security Evaluation

2015 UTM MARKET SHARE IN CHINA BY CCID



تا سال ۲۰۱۶ میلادی، Venustech UTM برای ۶ امین سال متوالی صدر نشین بازار داخلی بوده است.

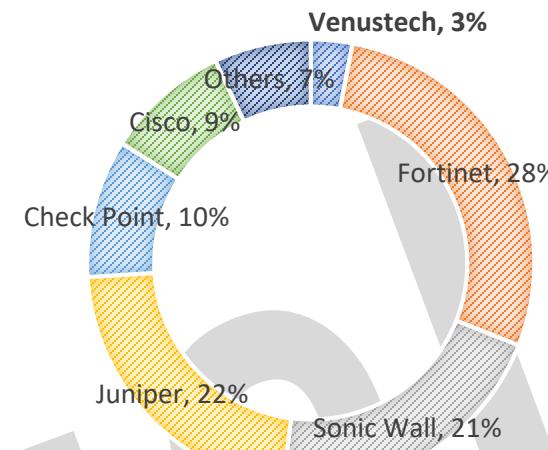
2014 UTM MARKET SHARE IN CHINA BY IDC



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

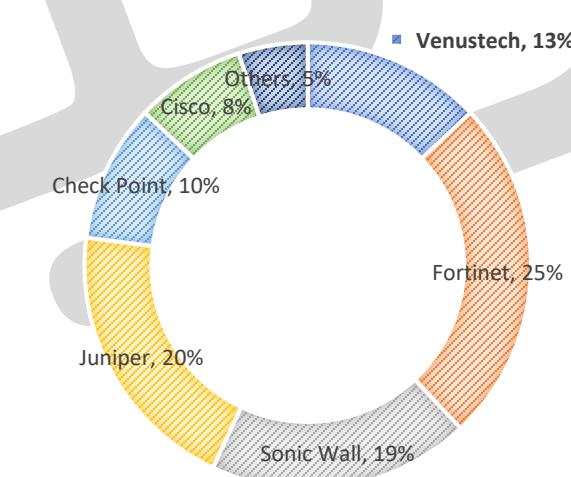
JAPAN SMB UTM MARKET SHARE 2014 BY FUJI CHIMERA

■ Venustech ■ Fortinet ■ Sonic Wall ■ Juniper ■ Check Point ■ Cisco ■ Others



JAPAN SMB UTM MARKET SHARE 2015 BY FUJI CHIMERA

■ Venustech ■ Fortinet ■ Sonic Wall ■ Juniper ■ Check Point ■ Cisco ■ Others



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

Route Security Rule NAT Rule DDoS Rule

Firewall

Strategy

Proxy

Domain

Address

Service

Time

Flow Control

Security Zone

Blacklist

Address Binding

Load Balance

Active Defense

Security Protection

Internet Behavior

Audit center

Session

IPv6

Unified Auth

CA Center

Vulnerability scan

Traffic State

State Monitor

Log&Report

Security rules configuration

*Rules name: pf1

*Serial number: 1

Source address:

Source port:

Source MAC:

Input security zone:

Strategy group: default

Destination address:

Time scheduling: any

Service:

Output security zone:

Comment:

Authentication user / User group

User / User group: Click to select

*Access control

Protection policy

Protocol control policy: NULL

Anti_virus policy: Standard_Virus_Prev

Invasion protection policy: Intrusion Detection

Internet behavior management policy: [Create EIM]

Cloud Policy: NULL

Audit policy: NULL

VIEW INFOMATION

VIEW INFOMATION

VIEW INFOMATION

VIEW INFOMATION

VIEW INFOMATION

VIEW INFOMATION

Mail delay audit:

Spam mail filter:

Flow control policy

Flow channel: NULL

Connection limit policy: NULL

VIEW INFOMATION

VIEW INFOMATION

Other configuration

Long connection: 0 minute(30-288000 minute,0 represents is not enabled)

Rules name consists of 1 to 32 letters,numbers,minus signs,Chinese and underlined

SUBMIT RETURN

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.

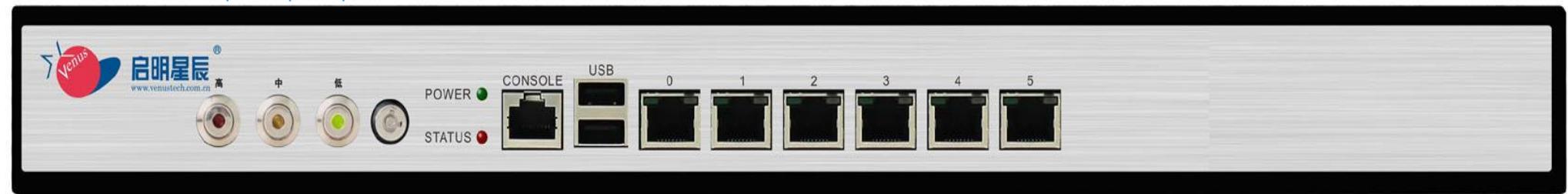
امکان استفاده از تنظیمات از پیش آماده شده

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)



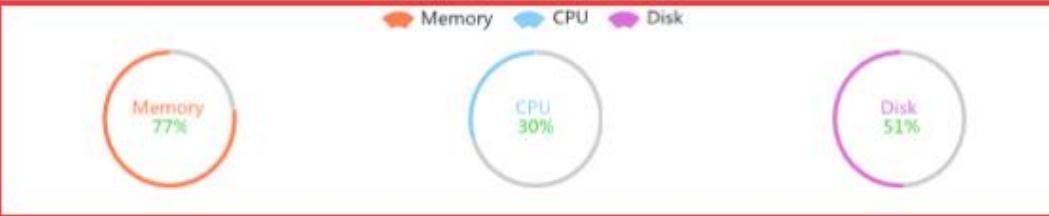
One touch configuration. Easy to use for specific customers.

Panel  Dashboard Latest Event

System information

Serial number	8e346f5f2b6a83d2
System startup time	2016/04/18 18:13:37
System datetime	2016/04/27 17:50:39
HA status	Stop
Host name	themis
Software version	V2.6
SSN	6.0.9
Hardware version	天博汉马USG一体化安全网关V2.6 USG-1000DP
Current administrator	administrator
	show

System resource



Memory 77% CPU 30% Disk 51%

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

کاربری آسان: نظارت بر منابع و ترافیک

Interface state

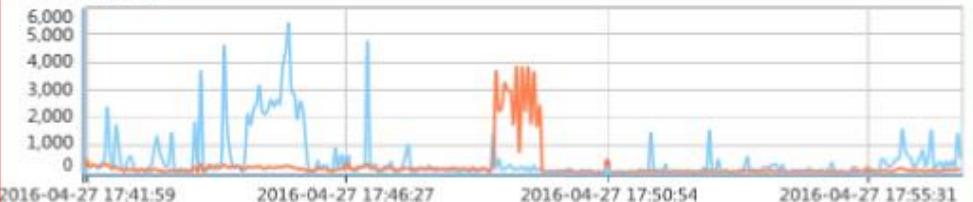


eth0 eth1 eth2 eth3 eth4 eth5

Interface Flow

in out

Rate(KB/s) (eth2)



2016-04-27 17:41:59 2016-04-27 17:46:27 2016-04-27 17:50:54 2016-04-27 17:55:31

Please select interface: **QUERY**

CLI console

```
ac>■
```

Local Engine

Kaspersky Engine

توانایی های پیش گیری از تهدیدات:
تشخیص ویروس

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

Virus Library

Version	1.3.0.3.405
<input checked="" type="radio"/> Regular virus library(Fast Scan)	
Number of Contained Features	
Description	<input checked="" type="checkbox"/> Standard engine <input checked="" type="checkbox"/> Enhanced engine
<input type="radio"/> 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.

Dual-engine mode

Local engine
This library includes the fastest top N viruses' signatures. It is suitable for the high performance.

Kaspersky engine
This library includes the latest top N viruses' signatures. 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

SMTP

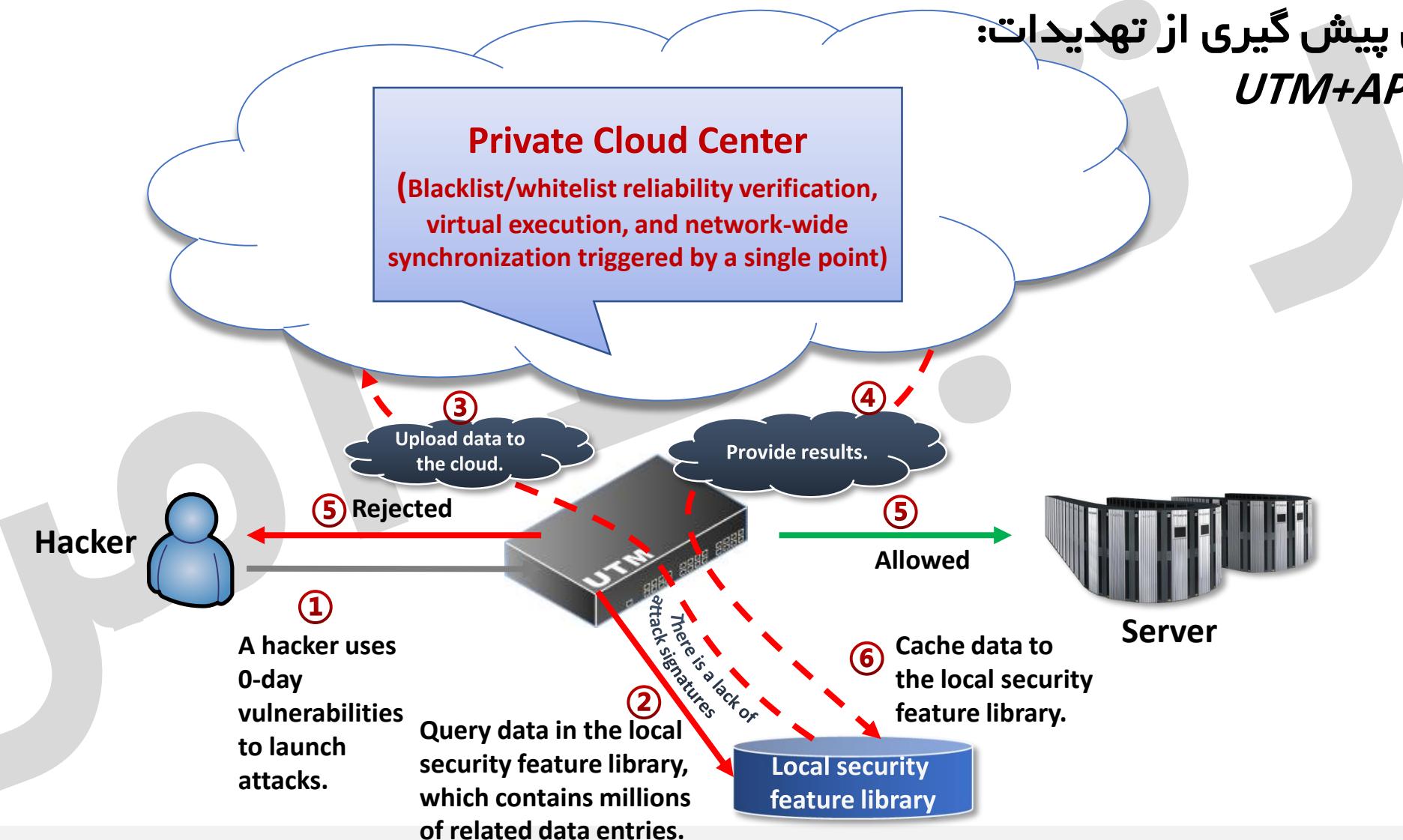
Isolation Time

10

minutes(0 is permanent)

APPLY

توانایی های پیش گیری از تهدیدات: *UTM+APT solution*



Scan Configuration Scan Status Scan Result

Scan Configure

Scan Strategy

- *Destination Address : test (Please use the address section in New Address)
- The Number of Concurrent Host Scanning : 10
- Automatic generation of security policy :

Plugin Type

All	Plugin Type	Description
<input checked="" type="checkbox"/>	ADX local security check	AIX (a UNIX system developed by IBM) local security check
<input checked="" type="checkbox"/>	Back Door	The attacker can use this kind of holes for host permissions
<input checked="" type="checkbox"/>	Exhaustive Attack	In turn try all possible keys to decrypt the ciphertext
<input checked="" type="checkbox"/>	CGI abuse	Code injection attacks on your browser
<input checked="" type="checkbox"/>	CGI abuseXSS	Code Injection attacks on your interpreter of browser
<input checked="" type="checkbox"/>	CISCO	Related attack for CISCO equipment
<input checked="" type="checkbox"/>	Authentication	Attack on the user permissions
<input checked="" type="checkbox"/>	DataBase	Attack on the database
<input checked="" type="checkbox"/>	Debian	Debian local security check
<input checked="" type="checkbox"/>	Default Unix Accounts	Login to a remote host by Unix account
<input checked="" type="checkbox"/>	Denial of Service	Attack on the web server
<input checked="" type="checkbox"/>	Firewall	Attack on the firewall
<input checked="" type="checkbox"/>	FTP	To obtain host information via FTP
<input checked="" type="checkbox"/>	Get remote shell	Get remote shell version and trying to login shell
<input checked="" type="checkbox"/>	Get remote root	As root on the remote to attack
<input checked="" type="checkbox"/>	Ordinary	Other vulnerabilities
<input checked="" type="checkbox"/>	Gentoo	Gentoo local security check hole
<input type="checkbox"/>	Test task	Vulnerabilities recognized with this last task

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

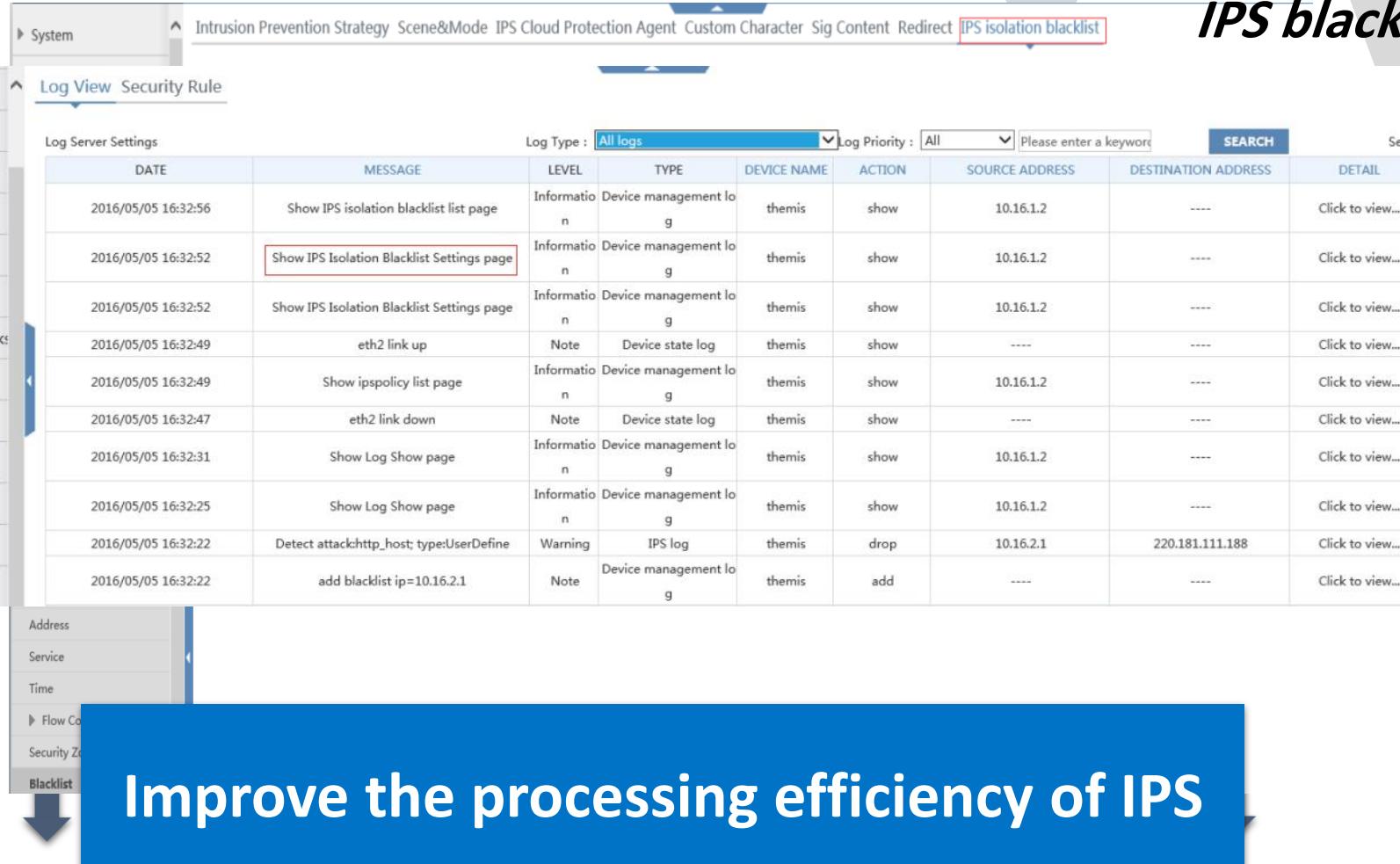
Intrusion Prevention Strategy

ID	NAME	TYPE	COMMENT	OPERATION
1	Standard Intrusion Prevention Template	Template		View Policy Info
2	Intrusion Detection Template	Template		View Policy Info
3	Linux Intrusion Prevention Template	Template		View Policy Info
4	\Windows Intrusion Prevention Template	Template		View Policy Info
5	scanPS20160427151252_001	Policy		Edit Delete

Security Rule NAT Rule DDoS Rule

SERIAL NUMBER	RULES NAME	SOURCE ADDRESS	DESTINATION ADDRESS	INPUT SECURITY ZONE	OUTPUT SECURITY ZONE	SERVICE	ACTION	EFFECT	HIT	STRATEGY GROUP	OPERATION
1	p1	any	none	none	any	any	Permit	0	0	default	Edit Delete
2	scan20160427151252_001	any	scan20160427151252_001	none	none	any	Permit	0	0	recommend	Edit Delete

توانایی های پیش گیری از تهدیدات: *IPS blacklist linkage*



Intrusion protection

Log View Security Rule

Log Server Settings

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
Flow Co
Security Z
Blacklist

Improve the processing efficiency of IPS

Office network

توانایی های پیش گیری از تهدیدات: Anti-DDoS

**Fine grained
detection
algorithm**

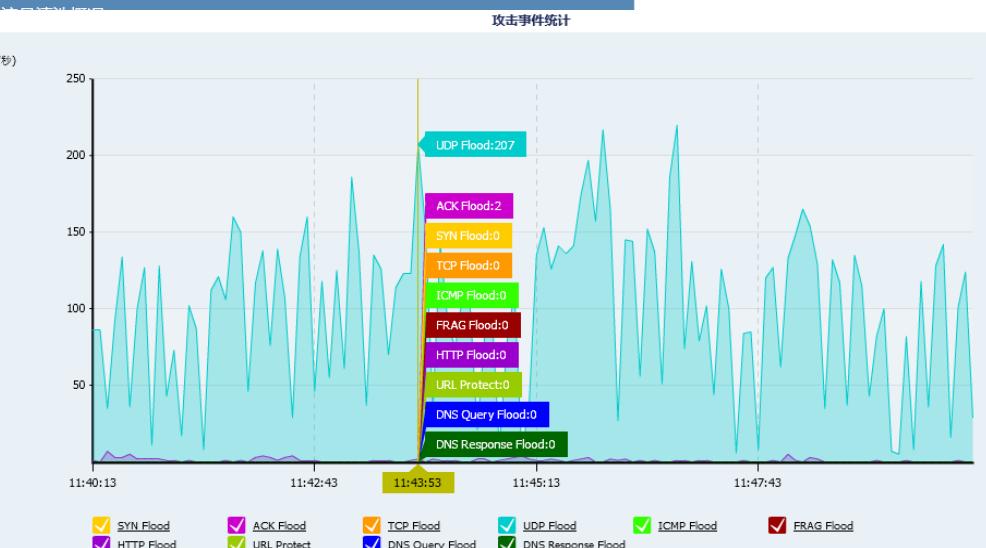
**Global
configuration**

**Attack traffic
statistic**

DNS Flood algorithm parameters	
Request source IP speed limit	500 (0-65535 pps)
Response source IP speed limit	500 (0-65535 pps)
The characteristics of filtration coefficient	
The clustering speed limit coefficient	
Retransmission detection	
Maximum passing packets detected	
Retransmission detection timeout	
Request characteristics filtering	
HTTP Flood algorithm parameters	
GET source IP threshold of sp... it	
POST source IP threshold of s... mit	
ICMP Flood algorithm parameters	
Fragment packets pass rate	10 % (0-100, default 10, 0 means unlimited)
Allow ping packets through	
Whitelist timeout	
Whitelist credibility	
Filter extra long ping packets	
Filter length	50000 (74-65535 Byte)
Maximum back-exploration time	
Strict inspection	

*The configuration take effect overall, is not affected by attack approach

- Anti address deceive attack
- Anti routing attack
- Anti Smurf attack
- Anti LAND attack
- Anti Winnuke attack
- Anti Queso scanning
- Anti SYN/FIN scanning
- Anti NULL scanning
- Anti Christmas tree attack



توانایی های پیش گیری از تهدیدات: URL self-learning

URL Policy Custom URL URL Config URL List Intelligent Learning Learning Result URL Config URL List Intelligent Learning Learning Result

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

URL config

URL recognition

Enable Intelligent recognition feature lib cache

Server ip

Server port

30 (Range:11-100M)

User self-service-extendable URL library

Enable IP address access is prohibited

Enable

SUBMIT



Office network

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

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)

Query Results of All Online Behavior

User Name	Group Name	Host IP	Dest IP	Port	Protocol	Time
11 chenkin	/root/test	192.168.84.128		220.11	tcp	2016-04-27 15:38:23
12 chenkin	/root/test	192.168.84.128		220.11	tcp	2016-04-27 15:38:23
13 baibing	/root/test2	192.168.84.50		192.11	tcp	2016-04-27 15:38:23
14 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23
15 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23
16 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23
17 chenkin	/root/test	192.168.84.128		220.11	tcp	2016-04-27 15:38:23
18 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23
19 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23
20 chenkin	/root/test	192.168.84.128		121.11	tcp	2016-04-27 15:38:23

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)

Mail

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

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 Succes	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 Succes	2016-04-27 15:38:23
33 截图	黄清	=liurr=	Receive Email		192.168.84.56	/root/test	Send or Receive Succes	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 Succes	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 Succes	2016-04-27 15:38:23
36 11000J测试进展反馈 已完成: 3类口的UDP吞	weiwd@leadsec.com.cn 董倚楠		Receive Email		192.168.84.56	/root/test	Send or Receive Succes	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.com	Send Email	xieqi		/root/test		Send or Receive Succes	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 Succes	2016-04-27 15:35:37
39 11000J测试进展反馈 已完成: 3类口的UDP吞	weiwd@leadsec.com.cn dongnn@leadsec.com	Send Email	weiwd		/root/test2/test3		Send or Receive Succes	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 Succes	2016-04-27 15:29:08

Displaying 31 to 40 of 166 items

192.168.84.56 2016-04-27 15:38:23

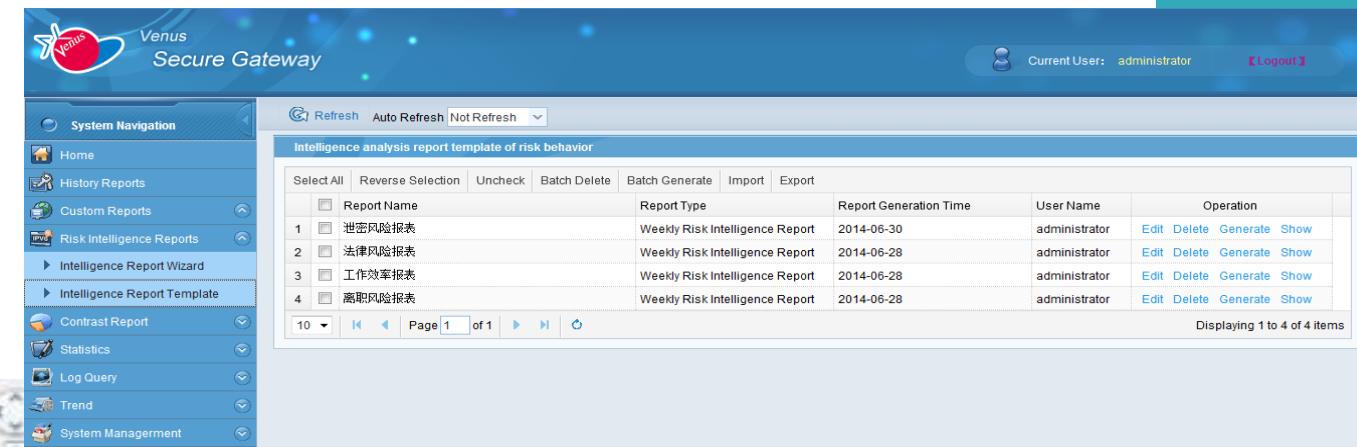
Email From: Mantis Bug Tracker <mantis@leads Email To: liurr@leadsec.com.cn
 Email Header: [3.6.0.9升级包定制版本测试 0043506]: [3.6.0.9(43226)UP-g-05-3.6.0.9-1功能升级包_HA]会话保护模式的配置同步，应用防护垃圾邮件配置两台...

Download original email

Email Content

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

Attachment Number: 0



Venus Secure Gateway

System Navigation

- Home
- History Reports
- Custom Reports
- Risk Intelligence Reports
- Intelligence Report Wizard
- Intelligence Report Template
- Contrast Report
- Statistics
- Log Query
- Trend
- System Management
- Event Map

Intelligence analysis report template of risk behavior

Report Name	Report Type	Report Generation Time	User Name	Operation
泄密风险报表	Weekly Risk Intelligence Report	2014-06-30	administrator	Edit Delete Generate Show
法律风险报表	Weekly Risk Intelligence Report	2014-06-28	administrator	Edit Delete Generate Show
工作效率报表	Weekly Risk Intelligence Report	2014-06-28	administrator	Edit Delete Generate Show
离职风险报表	Weekly Risk Intelligence Report	2014-06-28	administrator	Edit Delete Generate Show

Displaying 1 to 4 of 4 items

Page 1 of 1

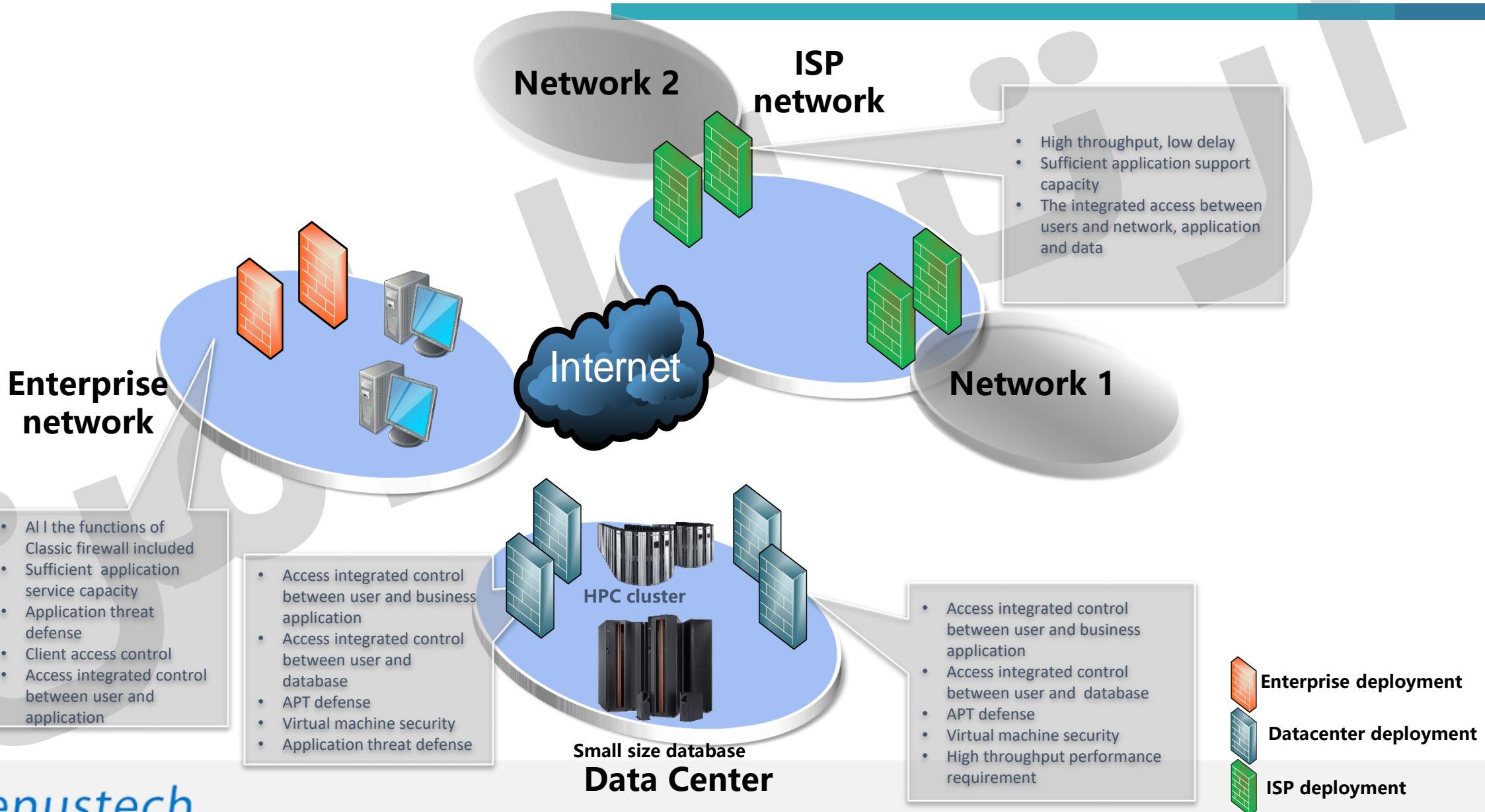


Beijing (116.3881,39.9299)

序号	城市名称	经度, 纬度	IP	事件IP	事件名称	次数
1	United States	(-97,38)	120.48.66	183.131.34.14	W EVENT	6
2	Japan	(139.89,36.08)	218.140.147.66	183.121.34.14	W EVENT	3
3	Taiwan	(121.23,24)	229.138.172.18	183.121.34.14	W EVENT	1
4	乌兰察布	(100.0107,47.9167)	302.170.01.100	183.131.34.13	W EVENT	1
5	鹤壁	(115.2775,39.6887)	120.0.49.66	183.131.34.14	W EVENT	1
6	Internal IP		192.168.0.38	183.131.34.14	W EVENT	1

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

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



مورد کاربرد ۱ : راه حل امنیتی شبکه خصوصی دولت

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

Target

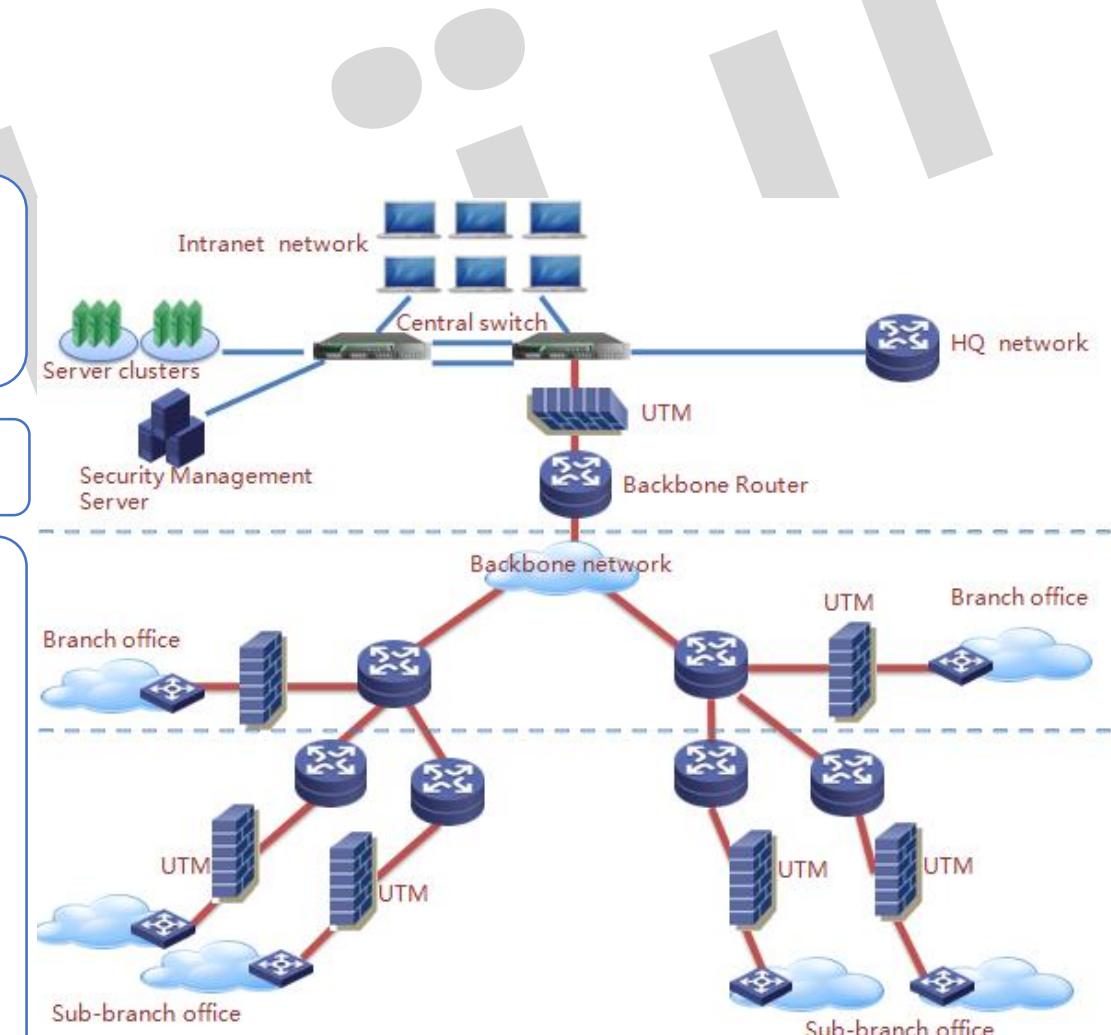
Considered the business ,geography location and administrative structure , the network is separated to several secure domain. Between the secure domains, the access control, intrusion and illegal access prevention, virus and worm prevention are properly realized.

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

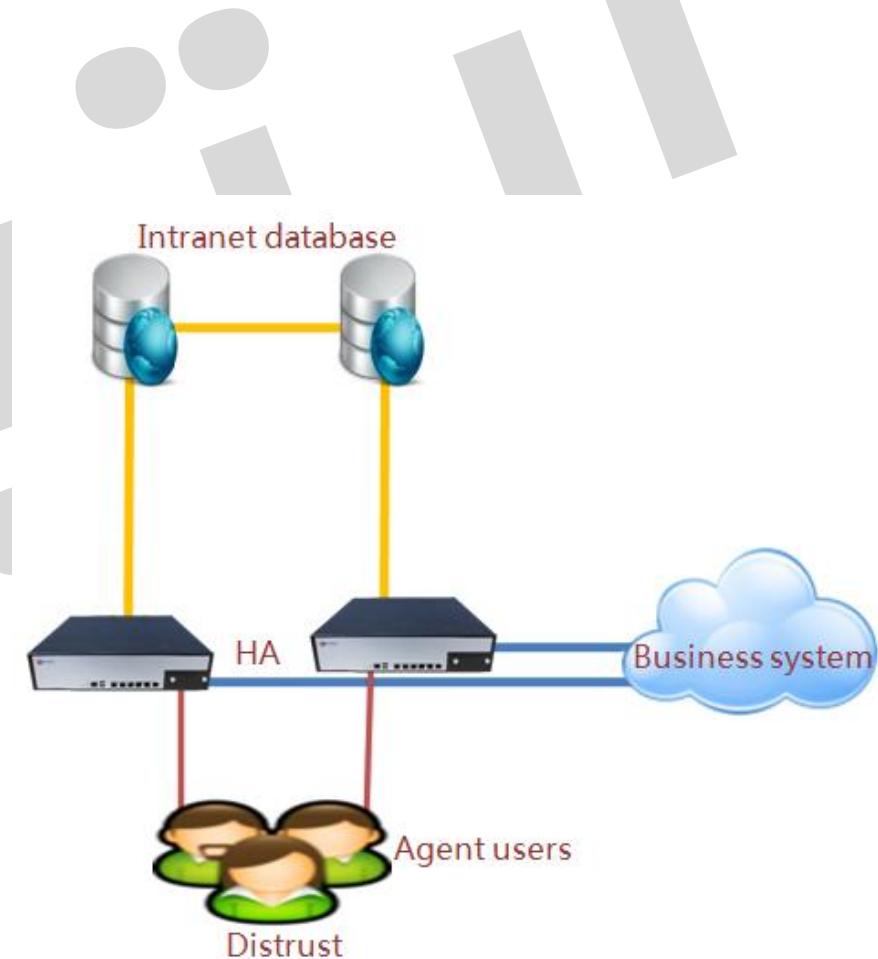
The data center is crucial for the business system of the ISP, but the client security is uncontrollable because of kinds of virus and worms spreading, therefore, it is vital to solve the secure issue at the client side to guarantee the security of the entire business system.

Scale

The core business system of the ISP is responsible for accounting and service fulfillment, the client sum is more than 10000.

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.





Thank you