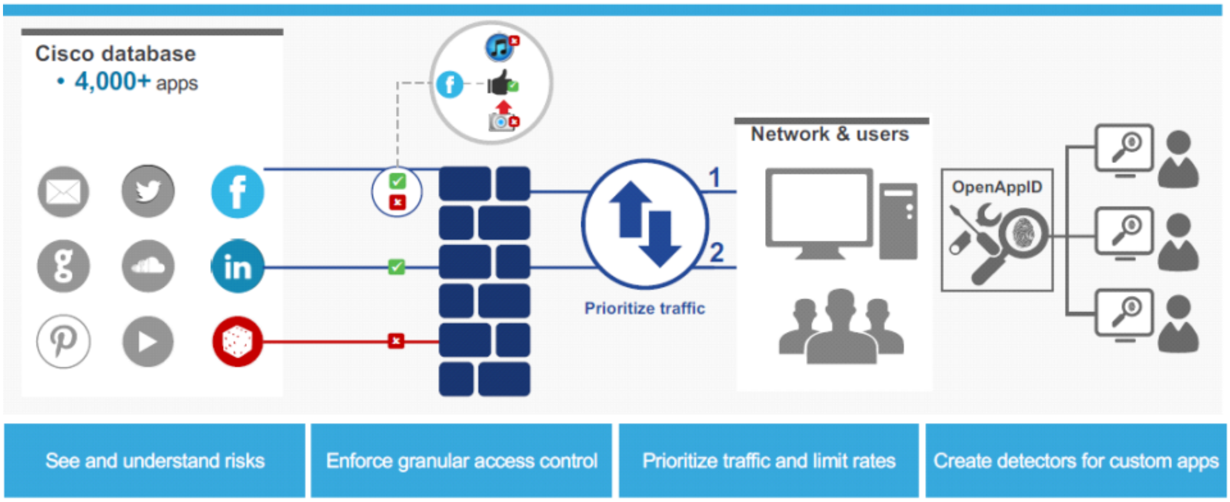
25：Discovery & Control Application

2020年1月17日 16:50

目录

1：发现&控制应用介绍



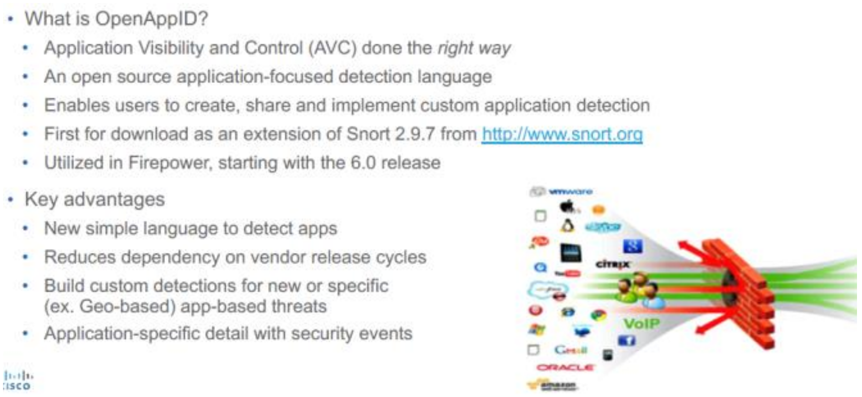
Cisco database
• 4,000+ apps
1
2
Prioritize traffic
Network & users
OpenAppID
See and understand risks
Enforce granular access control
Prioritize traffic and limit rates
Create detectors for custom apps

Firepower系统可以自动发现网络中运行的APP。可以识别哪些主机和用户运行特定应用。FTD可以通过（不通过）扫描器来发现网络应用。FTD可以实现用户可能会运行的应用程序类型进行APP过滤阻塞流量。

1.1：应用检测器

Firepower使用应用检测器识别网络上所运行的APP，检测公网根据检测器来源有所不同，主要检测器有两种

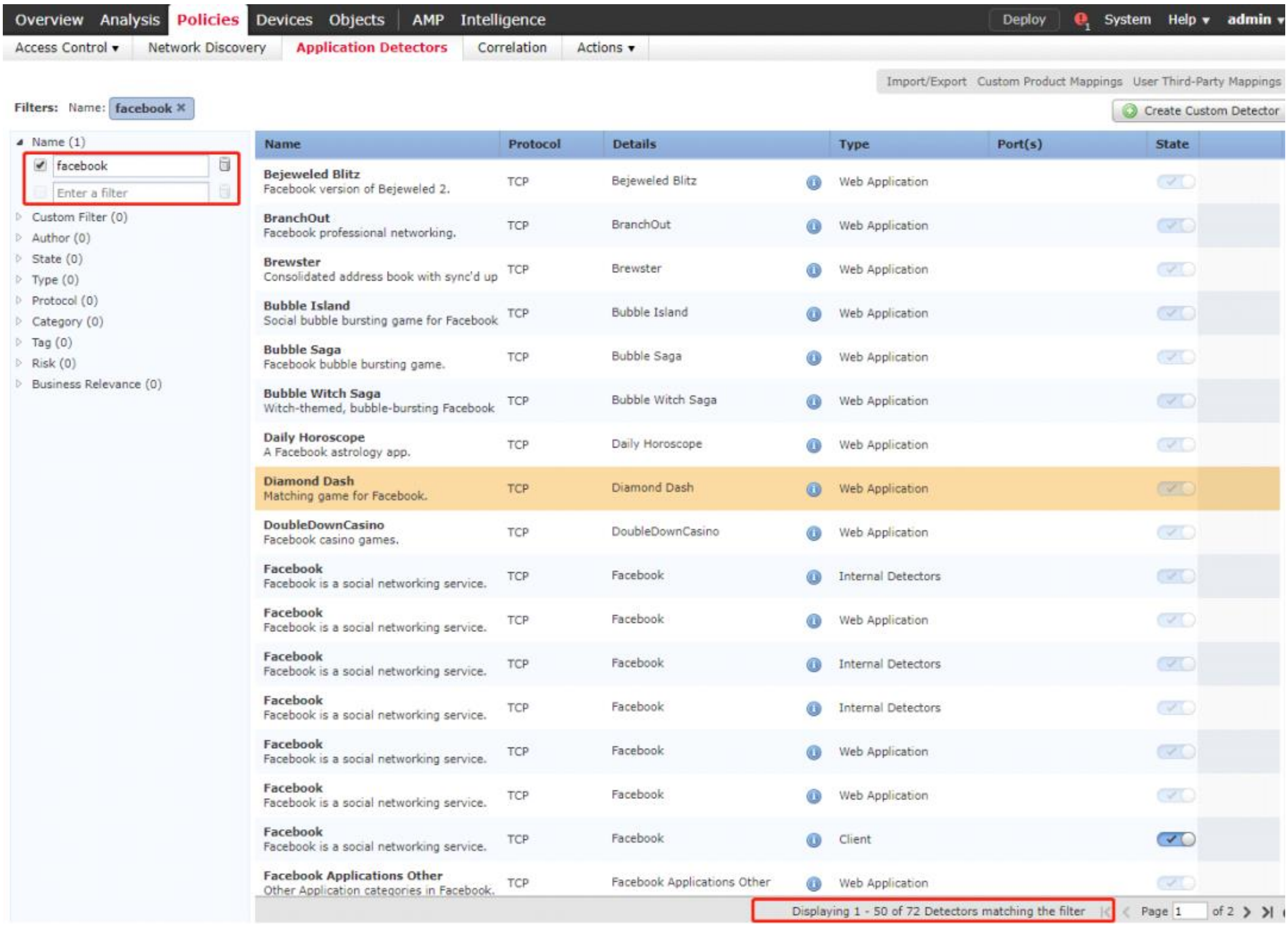
- System-provided detectors：默认Firepower软件中自带一组应用检测器。但想要精确检测最新的APP，需要对VDV（漏洞数据库）进行更新。（VDB中包含各种应用，操作系统和客户端软件的指纹，并记录已知漏洞，当Firepower检测到APP时可以将APP关联至已知漏洞，检测对网络的影响）
- User-created detectors：用户可以基于观察到的APP创建检测器，FMC可以未自定义的检测器提供全面管理控制，可以修改/禁用。后台其实是OpenAPPID（这是一个开源的应用检测模块）



- What is OpenAppID?
  - Application Visibility and Control (AVC) done the *right way*
  - An open source application-focused detection language
  - Enables users to create, share and implement custom application detection
  - First for download as an extension of Snort 2.9.7 from http://www.snort.org
  - Utilized in Firepower, starting with the 6.0 release
- Key advantages
  - New simple language to detect apps
  - Reduces dependency on vendor release cycles
  - Build custom detections for new or specific (ex. Geo-based) app-based threats
  - Application-specific detail with security events

若监控网络中主机连接非监控网络的服务器时，FMC使用客户端软件的信息推测应用协议

可以看到，FMC的APP Detectors检测到72个与Facebook相关的检测器。检测器的总数量取决于VDB的版本



Filters: Name: facebook ✕

- Name (1)
  - ☑ facebook
  - □ Enter a filter
- Custom Filter (0)
- Author (0)
- State (0)
- Type (0)
- Protocol (0)
- Category (0)
- Tag (0)
- Risk (0)
- Business Relevance (0)

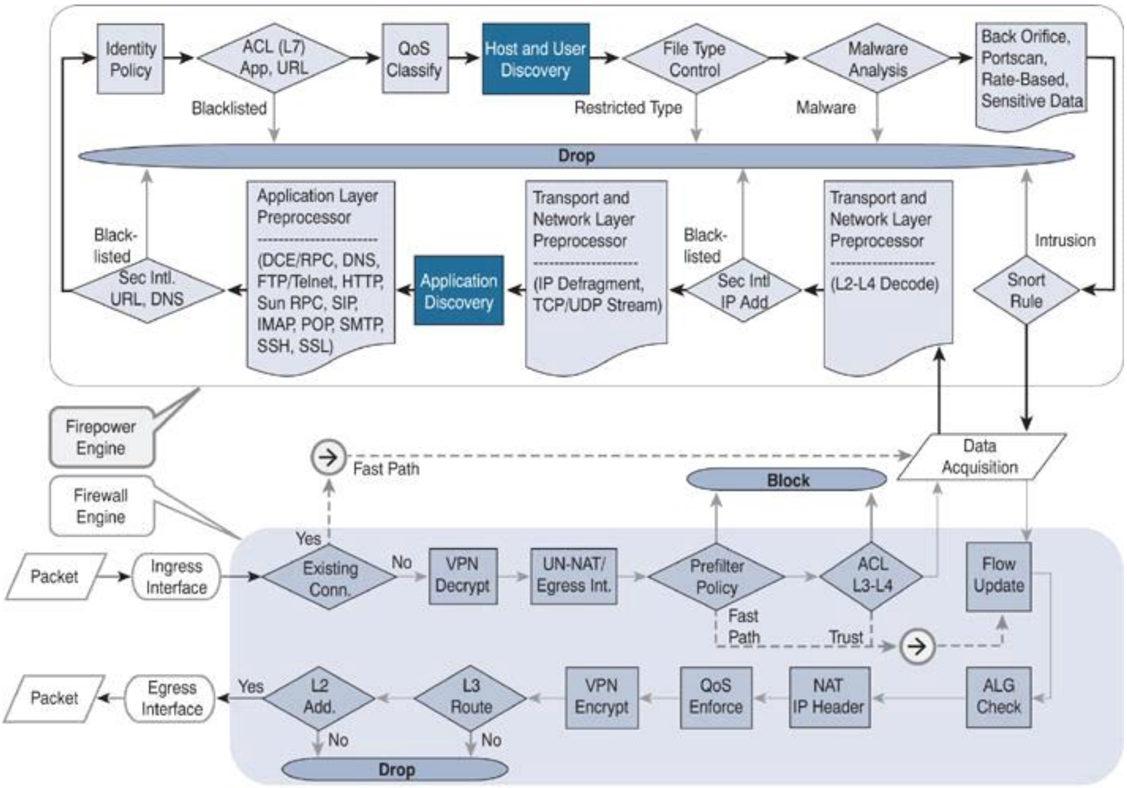
Name	Protocol	Details	Type	Port(s)	State
Bejeweled Blitz Facebook version of Bejeweled 2.	TCP	Bejeweled Blitz	Web Application		
BranchOut Facebook professional networking.	TCP	BranchOut	Web Application		
Brewster Consolidated address book with sync'd up	TCP	Brewster	Web Application		
Bubble Island Social bubble bursting game for Facebook	TCP	Bubble Island	Web Application		
Bubble Saga Facebook bubble bursting game.	TCP	Bubble Saga	Web Application		
Bubble Witch Saga Witch-themed, bubble-bursting Facebook	TCP	Bubble Witch Saga	Web Application		
Daily Horoscope A Facebook astrology app.	TCP	Daily Horoscope	Web Application		
Diamond Dash Matching game for Facebook.	TCP	Diamond Dash	Web Application		
DoubleDownCasino Facebook casino games.	TCP	DoubleDownCasino	Web Application		
Facebook Facebook is a social networking service.	TCP	Facebook	Internal Detectors		
Facebook Facebook is a social networking service.	TCP	Facebook	Web Application		
Facebook Facebook is a social networking service.	TCP	Facebook	Internal Detectors		
Facebook Facebook is a social networking service.	TCP	Facebook	Internal Detectors		
Facebook Facebook is a social networking service.	TCP	Facebook	Web Application		
Facebook Facebook is a social networking service.	TCP	Facebook	Web Application		
Facebook Facebook is a social networking service.	TCP	Facebook	Client		✓
Facebook Applications Other Other Application categories in Facebook.	TCP	Facebook Applications Other	Web Application		

Displaying 1 - 50 of 72 Detectors matching the filter   Page 1 of 2

1.2：应用检测运行框架

- Client & Server之间建立受监控连接过程中，FTD若可以识别出会话中的应用，则可以对应用进行控制。
- 若想识别应用，FTD必须分析会话中前几个少量数据包，直到识别应用完成之前，FTD都不可以执行应用控制规则。
- 如果Prefilter policy或ACP的配置是阻塞特定流量，那么FTD不会使用network discovery policy评估流量

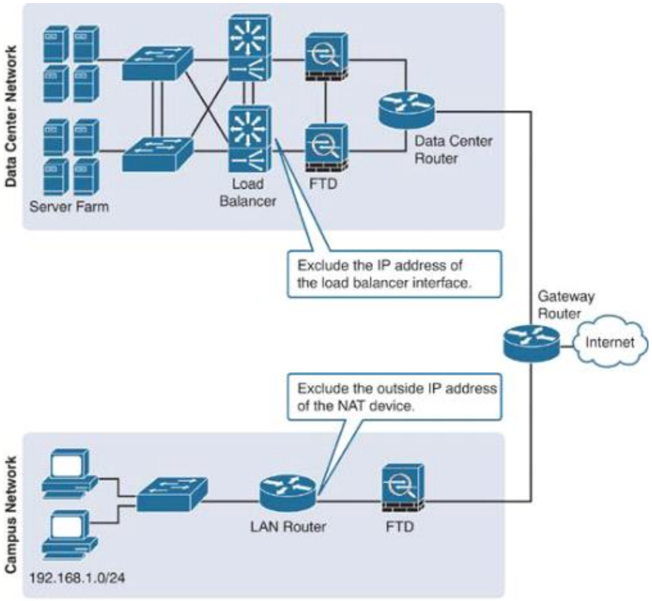
可以看到，只有通过SI策略才继续到达AVC（应用可视化控制）的模块



2：Best Practices

- 保持VDB版本最新，这样可以以更精确的版本信息检测最新的软件 ☆
- 默认FMC有部署APP Discovery策略，使用0.0.0.0/0和::/0为网络地址。这个地址可以确保Firepower系统从任何观察网络中发现APP。不要移除这个默认规则，因为Snort引擎会使用这个rule发现数据包来检测数据包的服务器元数据，以此进行入侵检测和防御 ☆
- 在配置Host/User发现策略的自定义规则时，确保添加自身网络已有IP地址段，不要选择0.0.0.0/0和::/0，这样会快速消耗host/user license
- 发现受监控网络中需要排除掉NAT的IP地址和用于负载均衡的IP以及公网地址，这类IP可能代表LAN中的多个计算机。当LAN活跃流量多时，FTD设备会有大量发现日志。排除掉可以提高设备性能☆

  举例说明：一个PC访问internet，internet的N地址没被发现策略排除，internet返回的流量会穿越FTD，FTD就也会发现internet的主机。

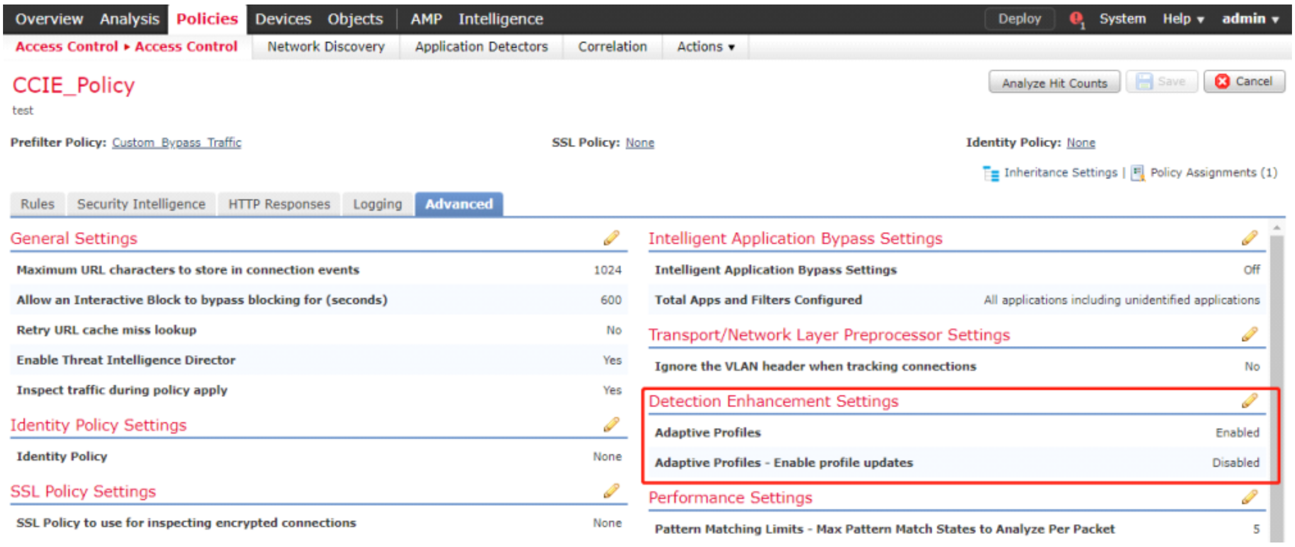


- 如果信任一些端口上运行的服务，那么可以在监控行为中排除掉一些端口，这样可以减少已知端口和服务发现的事件数量
- 避免创建重叠rule，不要多个rule有相同主机，防止性能过低
- 在尽可能靠近主机的地方部署FTD，FTD设备与host之间跳数越少，FTD检测到host的速度越快，信任度越高
- 默认网络发现规则发现所有网络的Application，所以没有特殊需求对于应用控制而言不需要额外配置网络发现策略
- 发现Application只是发现host&user附带的选项，除了默认策略之勾选发现Application，自定义规则都默认勾选发现APP
- 发现主机有限制数量，超过限制：可选行为，丢弃最早发现的host，或者丢弃新发现的host。默认=丢弃旧的host

Performance and Functionality	FMC 1600	FMC 2600	FMC 4600	FMCv
Maximum number of sensors managed	50	300	750	25* 10 2
Maximum IPS events	30 million	60 million	300 million	10 million
CPU	One Intel Xeon 4110 processor	Two Intel Xeon 4110 processors	Two Intel Xeon 4116 processors	-
Event storage space	900 GB	1.8 TB	3.2 TB	250 GB
Maximum network map size (hosts/users)	50,000/50,000	150,000/150,000	600,000/600,000	50,000/50,000

3：配置前提条件 ☆

- Firepower系统使用Adaptive Profiles（自适应配置文件）选项来执行应用控制。该选项可增强FTD检测能力，Adaptive profiles更新选项使用服务元数据，帮助FTD确定入侵规则是否与主机上运行的APP有关，并决定是否其启用这个规则（默认Adaptive profiles启用）


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▸ Access Control
Network Discovery
Application Detectors
Correlation
Actions ▾
Analyze Hit Counts
Save
Cancel
Inheritance Settings | Policy Assignments (1)
Rules Security Intelligence HTTP Responses Logging Advanced

CCIE_Policy

test

Prefilter Policy: Custom_Bypass_Traffic SSL Policy: None Identity Policy: None

General Settings

Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
Retry URL cache miss lookup	No
Enable Threat Intelligence Director	Yes
Inspect traffic during policy apply	Yes

Identity Policy Settings

Identity Policy	None

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections	None

Intelligent Application Bypass Settings

Intelligent Application Bypass Settings	Off
Total Apps and Filters Configured	All applications including unidentified applications

Transport/Network Layer Preprocessor Settings

Ignore the VLAN header when tracking connections	No

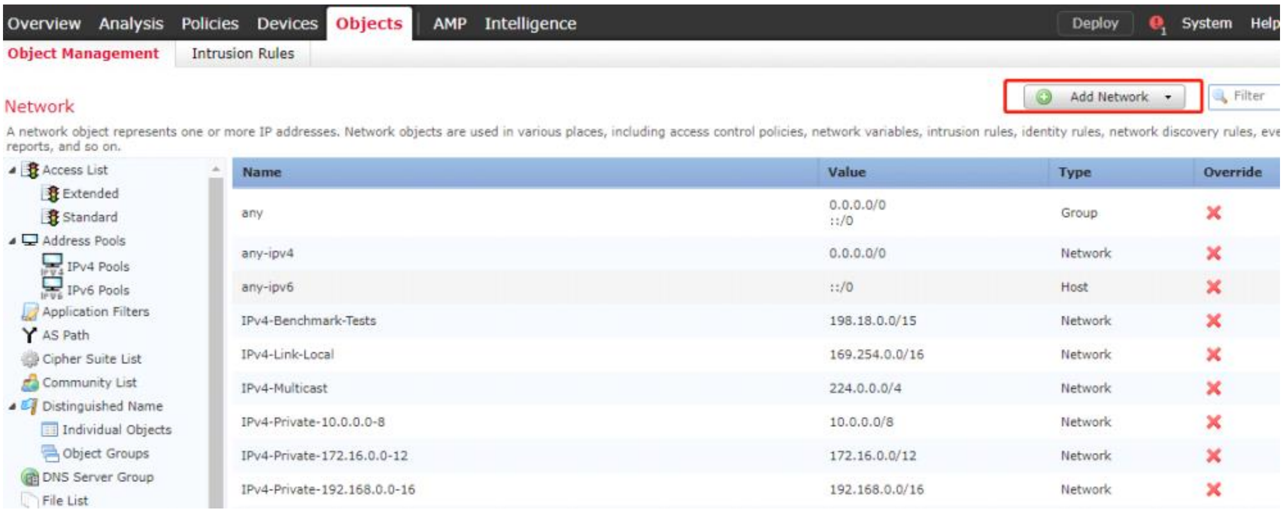
Detection Enhancement Settings

Adaptive Profiles	Enabled
Adaptive Profiles - Enable profile updates	Disabled

Performance Settings

Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5

- 为需要添加到Network discovery rule的网络地址创建object，这样方便调用



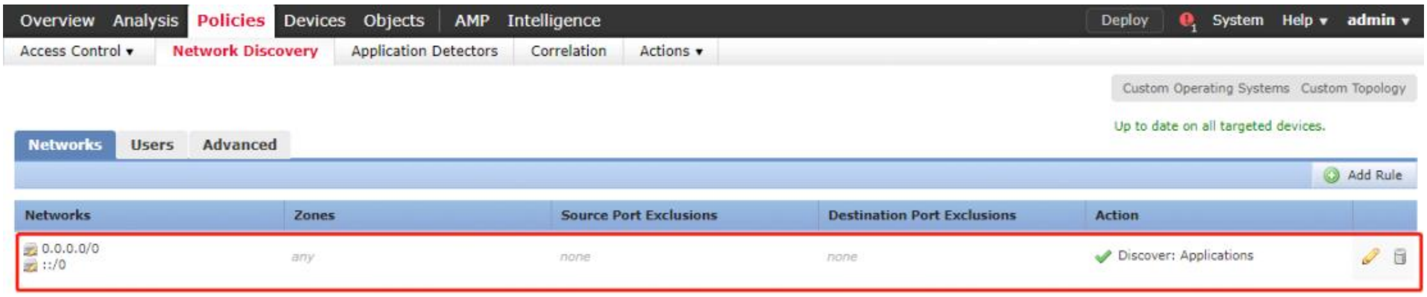
Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, eve reports, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	✗
any-ipv4	0.0.0.0/0	Network	✗
any-ipv6	::/0	Host	✗
IPv4-Benchmark-Tests	198.18.0.0/15	Network	✗
IPv4-Link-Local	169.254.0.0/16	Network	✗
IPv4-Multicast	224.0.0.0/4	Network	✗
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	✗
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	✗
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	✗

4：Config discovery Application

- 默认网络发现规则发现所有网络的Application
- 所以没有特殊需求对于应用控制而言不需要额外配置网络发现策略

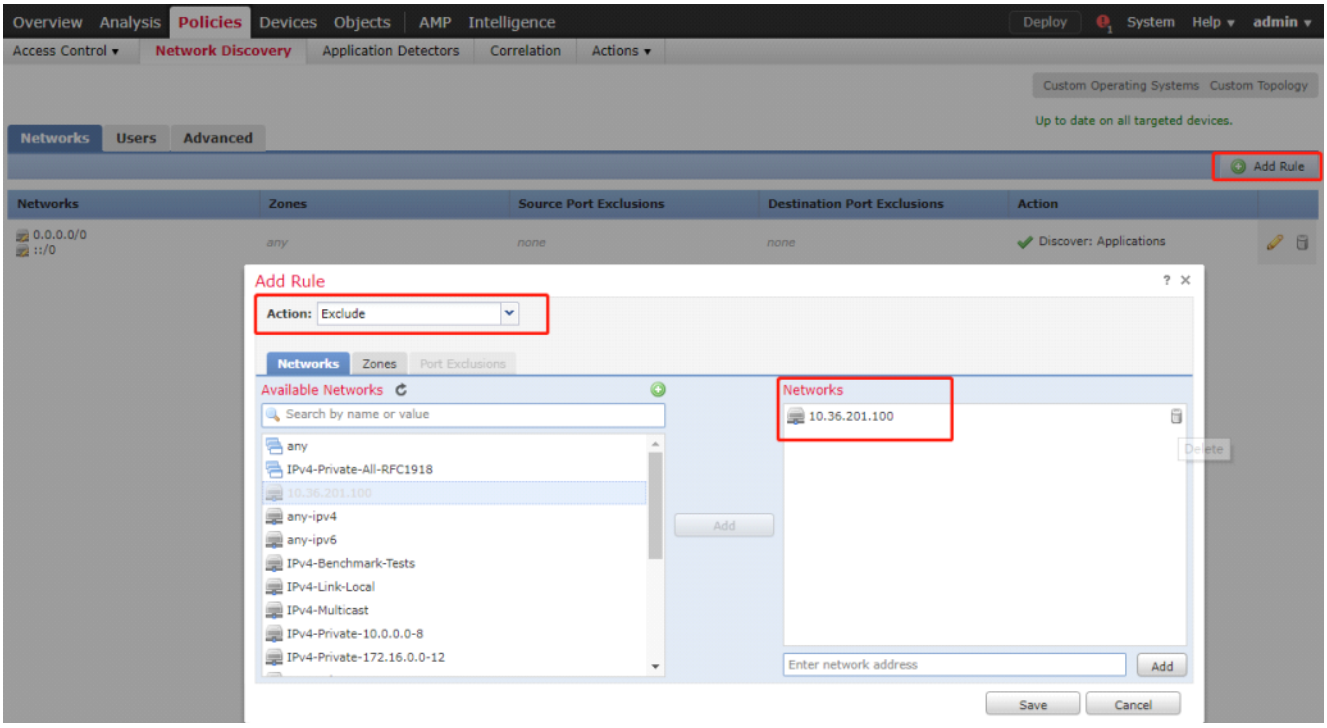

Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▾
Network Discovery
Application Detectors
Correlation
Actions ▾
Custom Operating Systems Custom Topology
Up to date on all targeted devices.
Networks Users Advanced
Add Rule

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

4.1：推荐排除NAT地址/负载均衡地址

若网络中有NAT设备，排除掉NAT的IP，避免发现事件居多影响性能。比如internet的主机返回内网主机流量会穿越FTD，这时候FTD也会

分析internet主机。



Up to date on all targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

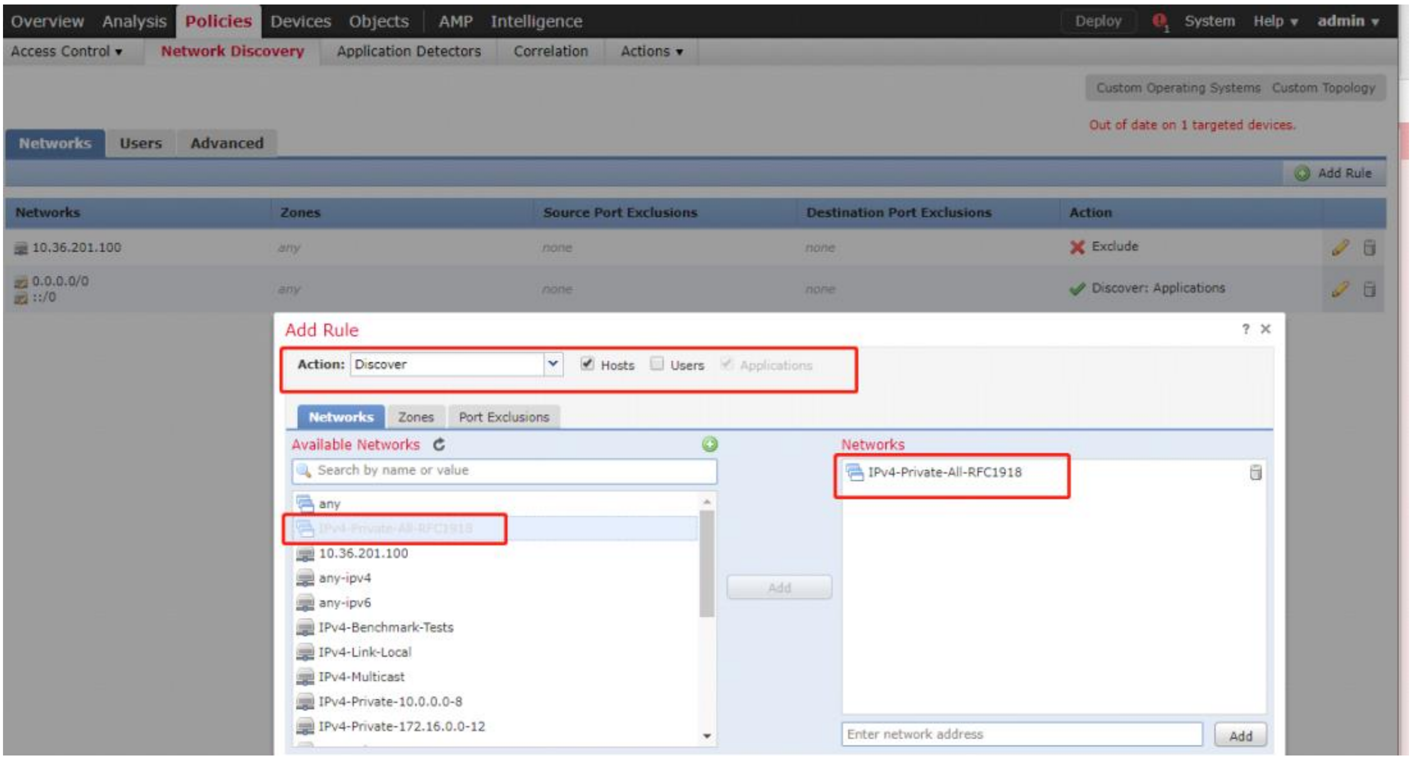
Add Rule

Action: Exclude

Networks: 10.36.201.100

4.2：创建一个自定义规则，发现指定网络运行的主机和应用

- 应用发现是发现User/Host发现自带的，没法选。
- Object选择RFC定义的三个私网地址段



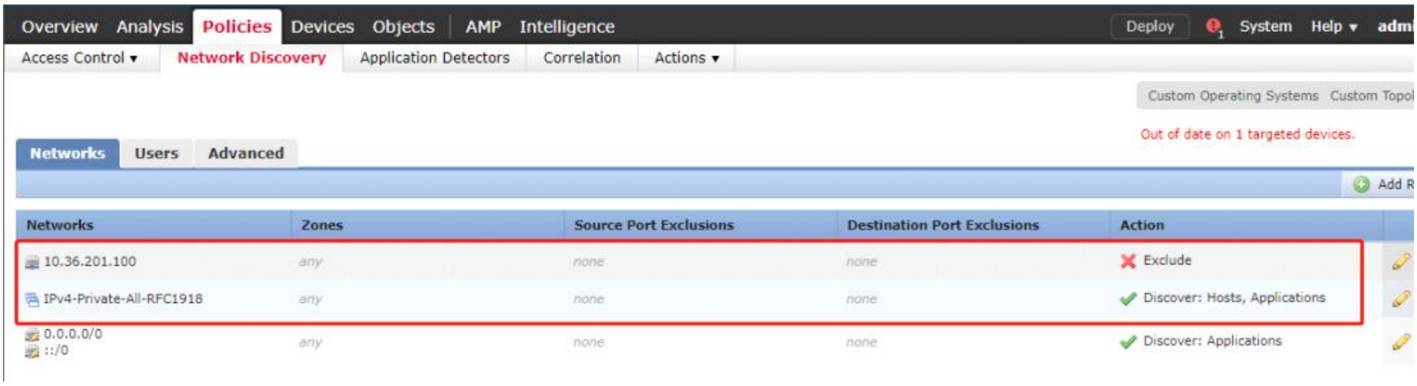
Out of date on 1 targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
10.36.201.100	any	none	none	✗ Exclude
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

Add Rule

Action: Discover ☑ Hosts ☐ Users ☑ Applications

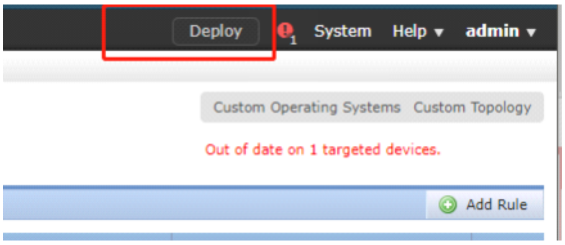
Networks: IPv4-Private-All-RFC1918



Out of date on 1 targeted devices.

Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
10.36.201.100	any	none	none	✗ Exclude
IPv4-Private-All-RFC1918	any	none	none	✓ Discover: Hosts, Applications
0.0.0.0/0 ::/0	any	none	none	✓ Discover: Applications

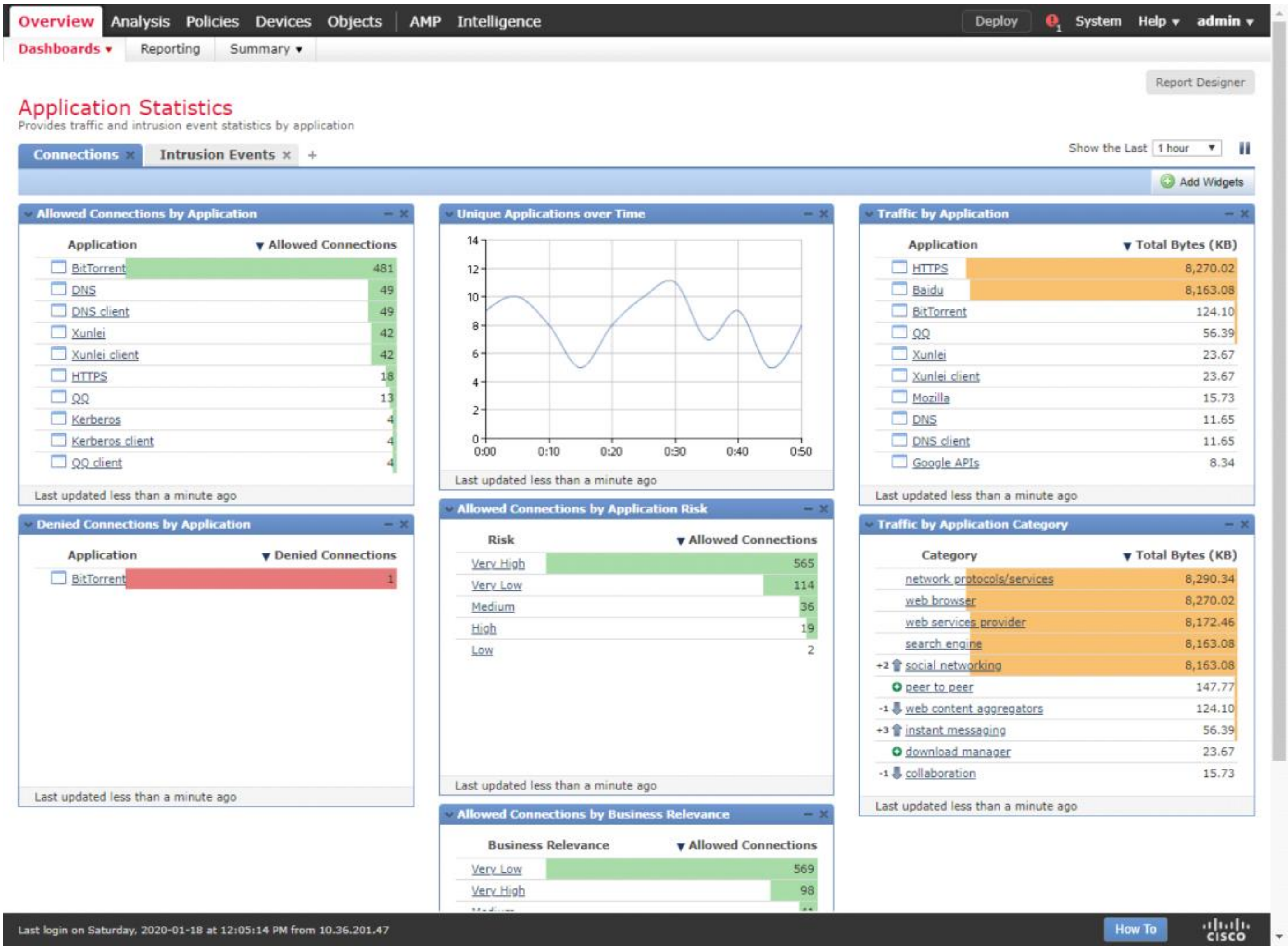
部署Deploy



Out of date on 1 targeted devices.

4.3：校验

当主机发起穿越FTD流量时，FMC的GUI可以看到发现事件



Application Statistics

Provides traffic and intrusion event statistics by application

Allowed Connections by Application

Application	▾ Allowed Connections
BitTorrent	481
DNS	49
DNS client	49
Xunlei	42
Xunlei client	42
HTTPS	18
QQ	13
Kerberos	4
Kerberos client	4
QQ client	4

Last updated less than a minute ago

Denied Connections by Application

Application	▾ Denied Connections
BitTorrent	1

Last updated less than a minute ago

Allowed Connections by Application Risk

Risk	▾ Allowed Connections
Very High	565
Very Low	114
Medium	36
High	19
Low	2

Last updated less than a minute ago

Allowed Connections by Business Relevance

Business Relevance	▾ Allowed Connections
Very Low	569
Very High	98

Traffic by Application

Application	▾ Total Bytes (KB)
HTTPS	8,270.02
Baidu	8,163.08
BitTorrent	124.10
QQ	56.39
Xunlei	23.67
Xunlei client	23.67
Mozilla	15.73
DNS	11.65
DNS client	11.65
Google APIs	8.34

Last updated less than a minute ago

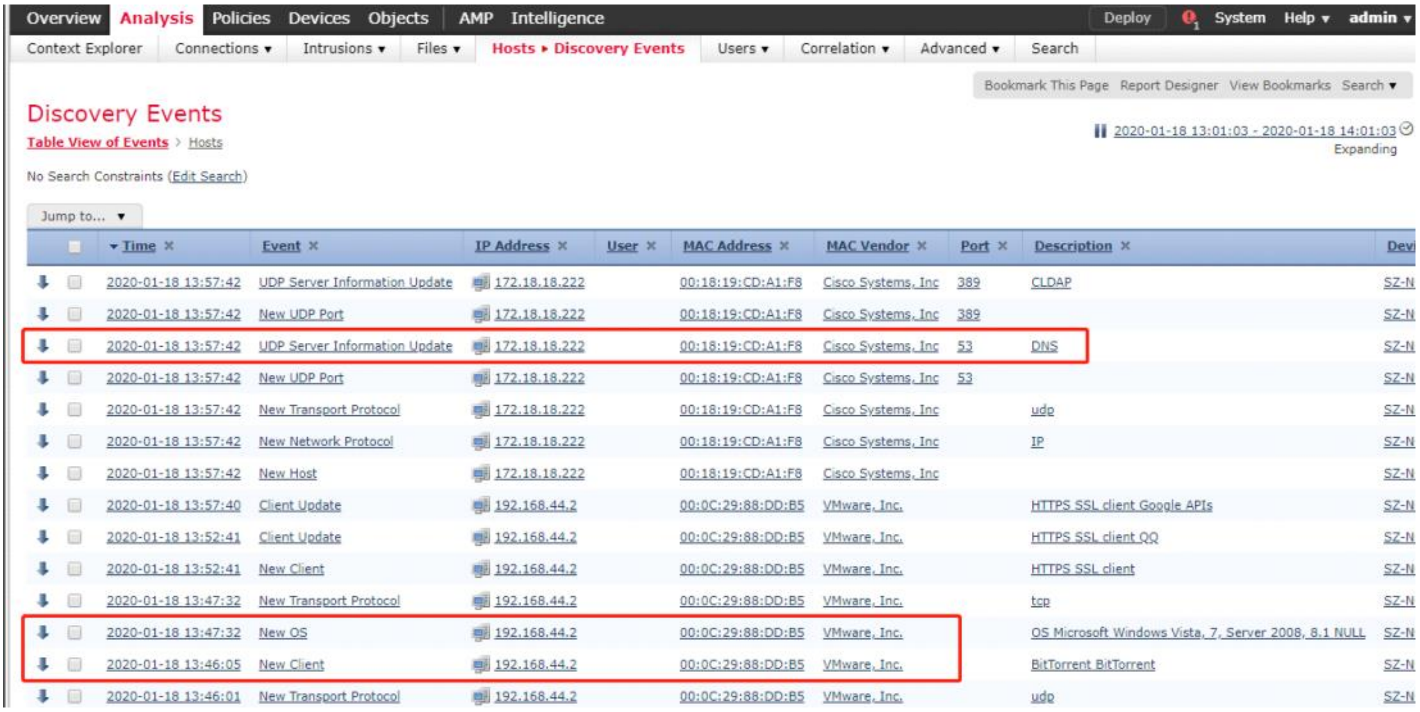
Traffic by Application Category

Category	▾ Total Bytes (KB)
network protocols/services	8,290.34
web browser	8,270.02
web services provider	8,172.46
search engine	8,163.08
+2 social networking	8,163.08
peer to peer	147.77
-1 web content aggregators	124.10
+3 instant messaging	56.39
download manager	23.67
-1 collaboration	15.73

Last updated less than a minute ago

Last login on Saturday, 2020-01-18 at 12:05:14 PM from 10.36.201.47

可以看到发现主机的应用，172.18.18.222是44.2的DNS服务器，所以回去流量会穿越FTD被扫到。



Discovery Events

Table View of Events > Hosts

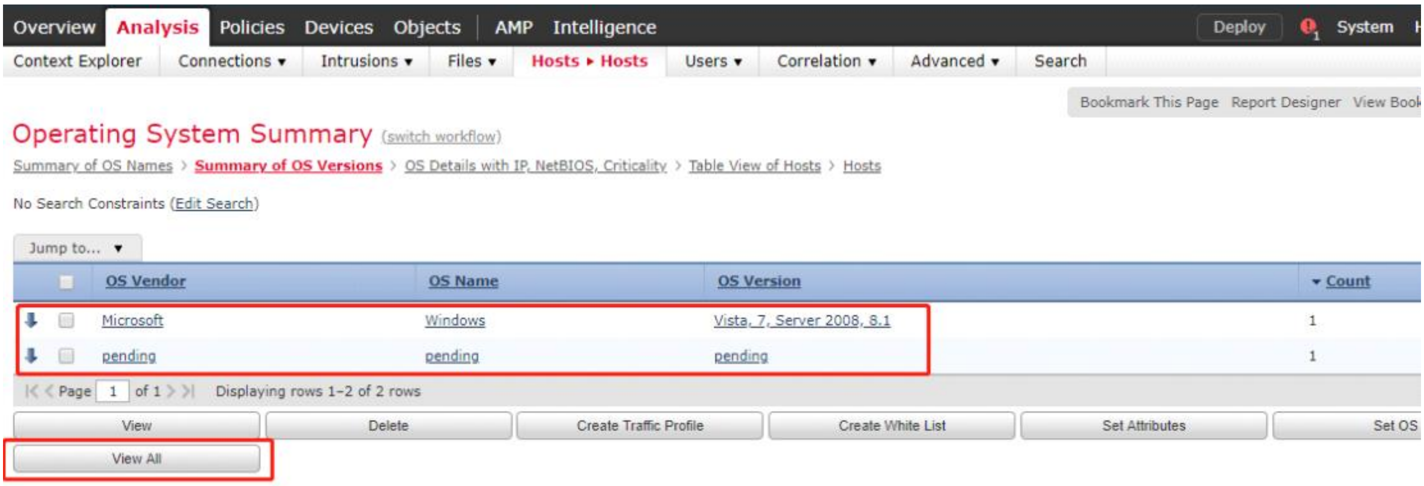
2020-01-18 13:01:03 - 2020-01-18 14:01:03
Expanding

No Search Constraints (Edit Search)

	□	Time	Event	IP Address	User	MAC Address	MAC Vendor	Port	Description	Devi
⬇	□	2020-01-18 13:57:42	UDP Server Information Update	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc	389	CLDAP	SZ-N
⬇	□	2020-01-18 13:57:42	New UDP Port	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc	389		SZ-N
⬇	□	2020-01-18 13:57:42	UDP Server Information Update	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc	53	DNS	SZ-N
⬇	□	2020-01-18 13:57:42	New UDP Port	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc	53		SZ-N
⬇	□	2020-01-18 13:57:42	New Transport Protocol	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc		udp	SZ-N
⬇	□	2020-01-18 13:57:42	New Network Protocol	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc		IP	SZ-N
⬇	□	2020-01-18 13:57:42	New Host	172.18.18.222		00:18:19:CD:A1:F8	Cisco Systems, Inc			SZ-N
⬇	□	2020-01-18 13:57:40	Client Update	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		HTTPS SSL client Google APIs	SZ-N
⬇	□	2020-01-18 13:52:41	Client Update	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		HTTPS SSL client QQ	SZ-N
⬇	□	2020-01-18 13:52:41	New Client	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		HTTPS SSL client	SZ-N
⬇	□	2020-01-18 13:47:32	New Transport Protocol	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		tcp	SZ-N
⬇	□	2020-01-18 13:47:32	New OS	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		OS Microsoft Windows Vista, 7, Server 2008, 8.1 NULL	SZ-N
⬇	□	2020-01-18 13:46:05	New Client	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		BitTorrent BitTorrent	SZ-N
⬇	□	2020-01-18 13:46:01	New Transport Protocol	192.168.44.2		00:0C:29:88:DD:B5	VMware, Inc.		udp	SZ-N

分析主机发现

- 因为我们创建了自定义host发现所有私网地址段的主机，Application是发现host自带的选项。
- 如果只是用default network discovery，那么只会发现APP。
- 可以看到，扫到两台。一台微软的windows，还有一台带待定还不能确认



Operating System Summary (switch workflow)

Summary of OS Names > Summary of OS Versions > OS Details with IP, NetBIOS, Criticality > Table View of Hosts > Hosts

No Search Constraints (Edit Search)

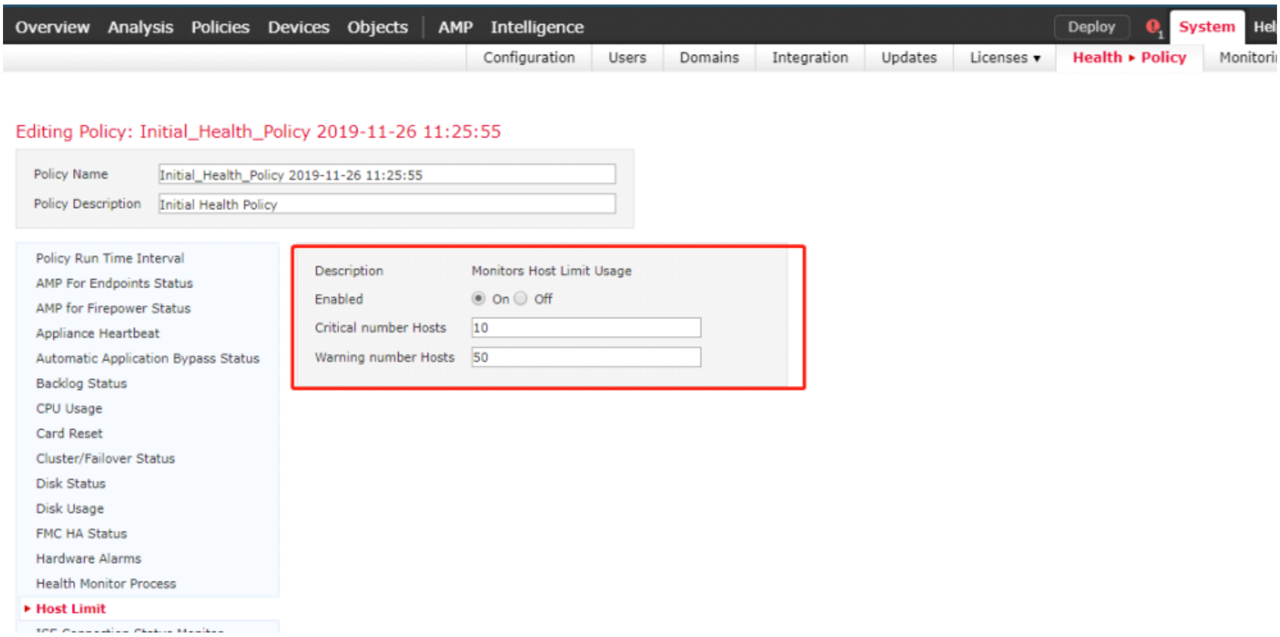
	□	OS Vendor	OS Name	OS Version	Count
⬇	□	Microsoft	Windows	Vista, 7, Server 2008, 8.1	1
⬇	□	pending	pending	pending	1

Page 1 of 1 Displaying rows 1-2 of 2 rows

4.4：排查未发现新主机

若有host没被FTD发现，则校验FMC是否有超过主机发现限制的告警，若希望看到告警需要开启健康监控

Performance and Functionality	FMC 1600	FMC 2600	FMC 4600	FMCv
Maximum network map size (hosts/users)	50,000/50,000	150,000/150,000	600,000/600,000	50,000/50,000



Editing Policy: Initial_Health_Policy 2019-11-26 11:25:55

Policy Name: Initial_Health_Policy 2019-11-26 11:25:55

Policy Description: Initial Health Policy

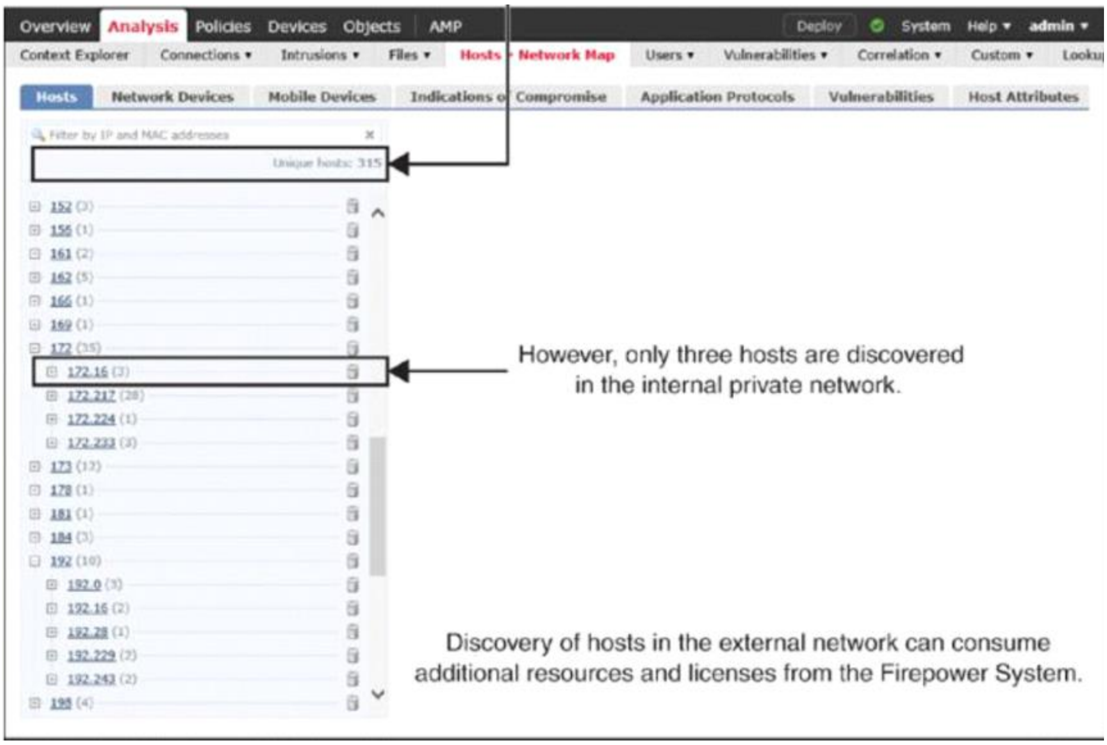
Description: Monitors Host Limit Usage

Enabled: ● On ○ Off

Critical number Hosts: 10

Warning number Hosts: 50

示例，由于host发现规则没有排除internet公网地址，那么FTD发现internet主机会占用资源和许可就像这张图，发现了315台，只有三台172的是FTD内网的主机，其余都是公网



Unique hosts: 315

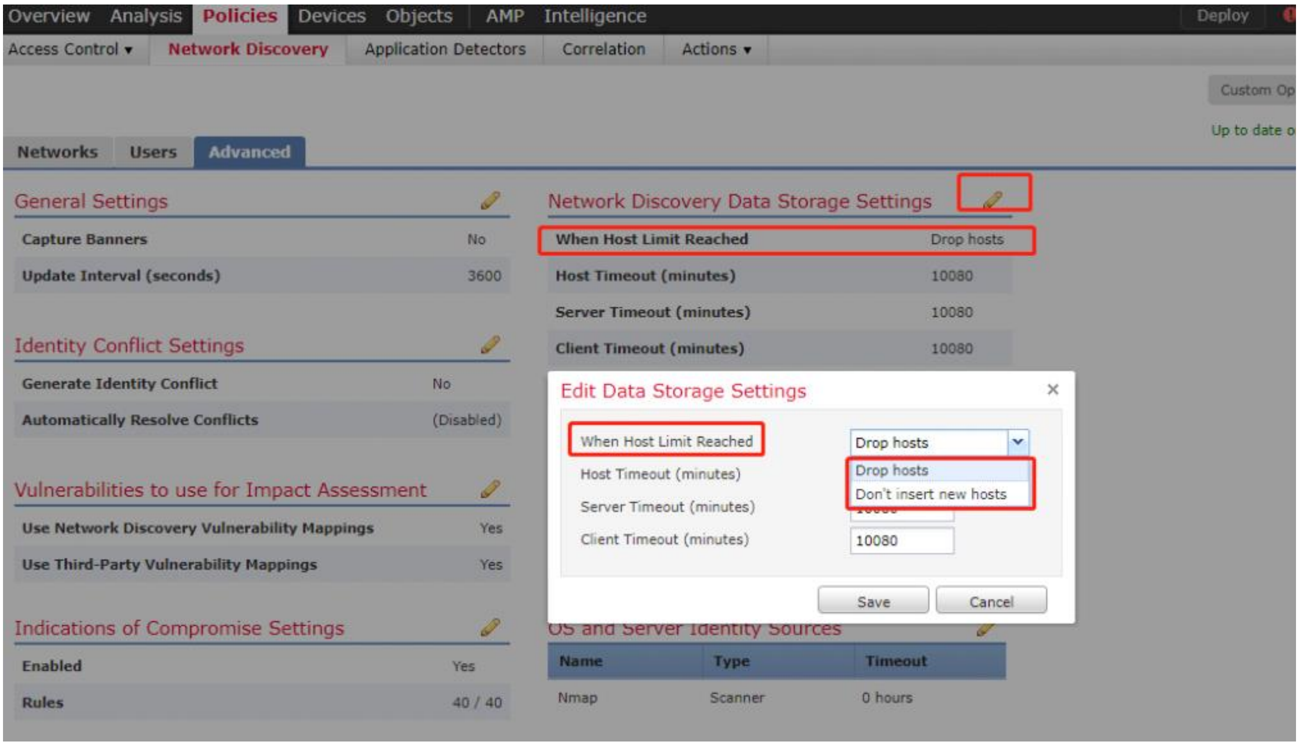
```
152 (3)
156 (1)
161 (2)
162 (5)
166 (1)
169 (1)
172 (35)
  172.16 (3)
  172.217 (28)
  172.224 (1)
  172.233 (3)
173 (13)
178 (1)
181 (1)
184 (3)
192 (10)
  192.0 (3)
  192.16 (2)
  192.28 (1)
  192.229 (2)
  192.243 (2)
198 (4)
```

However, only three hosts are discovered in the internal private network.

Discovery of hosts in the external network can consume additional resources and licenses from the Firepower System.

4.5：当FMC发现host数量超过上限时，修改行为

可选行为，丢弃最早发现的host，或者丢弃新发现的host，默认丢弃旧的host



General Settings

Capture Banners	No
Update Interval (seconds)	3600

Identity Conflict Settings

Generate Identity Conflict	No
Automatically Resolve Conflicts	(Disabled)

Vulnerabilities to use for Impact Assessment

Use Network Discovery Vulnerability Mappings	Yes
Use Third-Party Vulnerability Mappings	Yes

Indications of Compromise Settings

Enabled	Yes
Rules	40 / 40

Network Discovery Data Storage Settings

When Host Limit Reached	Drop hosts
Host Timeout (minutes)	10080
Server Timeout (minutes)	10080
Client Timeout (minutes)	10080

Edit Data Storage Settings

When Host Limit Reached	Drop hosts
Host Timeout (minutes)	Drop hosts Don't insert new hosts
Server Timeout (minutes)	
Client Timeout (minutes)	10080

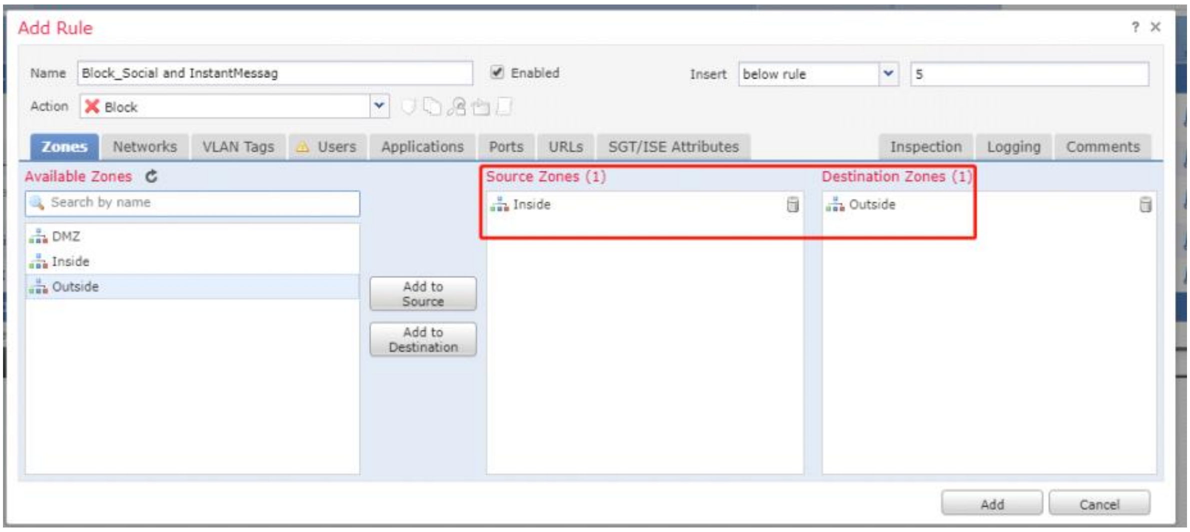
OS and Server Identity Sources

Name	Type	Timeout
Nmap	Scanner	0 hours

5：Block Application

5.1：配置ACR block Appication

配置源目zone


Add Rule

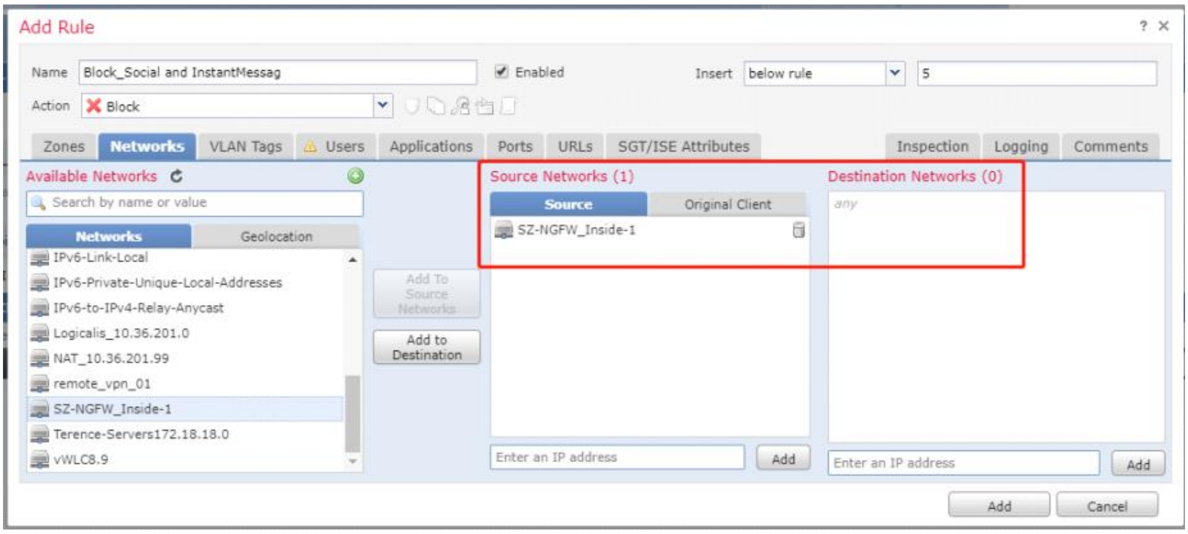
Name Block_Social and InstantMessag ☑ Enabled Insert below rule 5

Action Block

Source Zones (1): Inside

Destination Zones (1): Outside

配置源目地址段



Add Rule

Name: Block_Social and InstantMessag ☑ Enabled Insert: below rule 5

Action: Block

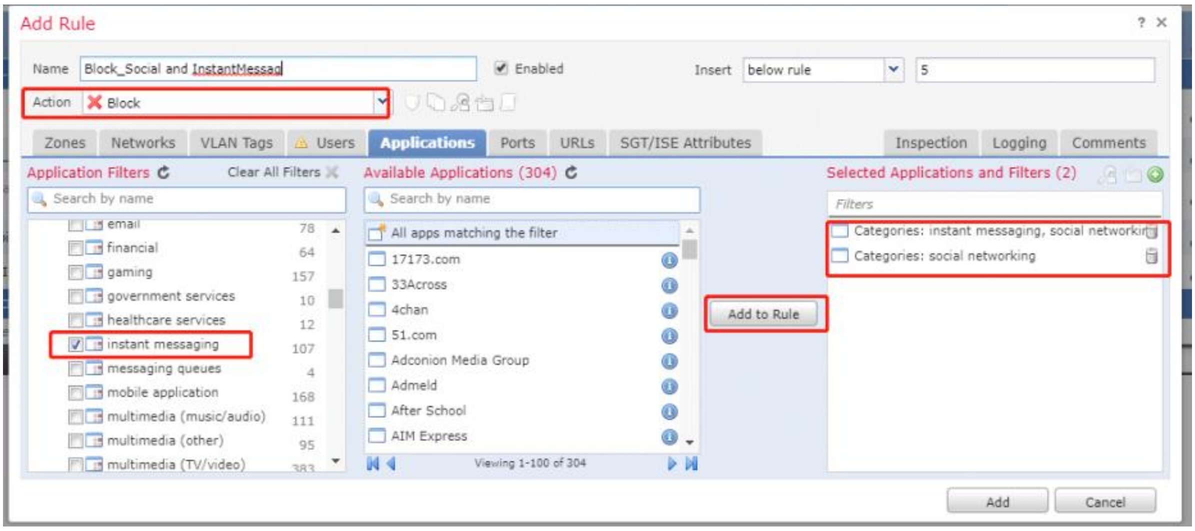
Source Networks (1)

Source: SZ-NGFW_Inside-1

Original Client

Destination Networks (0): any

配置Block即使通信和社交应用（QQ/微信/脸书等），也可以指定block某一个APP



Add Rule

Name: Block_Social and InstantMessag ☑ Enabled Insert: below rule 5

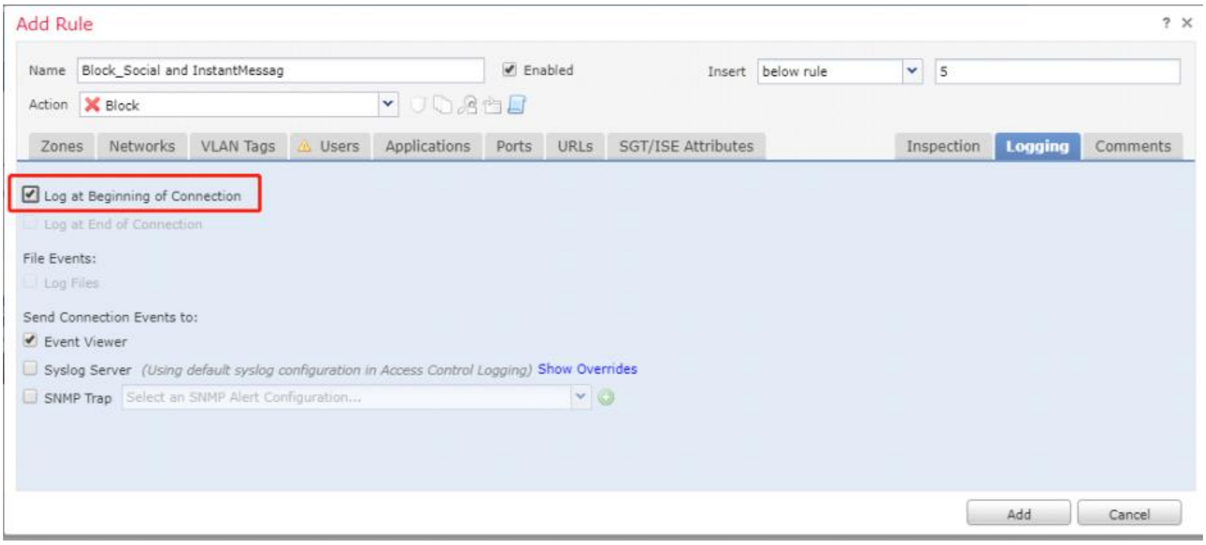
Action: Block

□ email	78
□ financial	64
□ gaming	157
□ government services	10
□ healthcare services	12
☑ instant messaging	107
□ messaging queues	4
□ mobile application	168
□ multimedia (music/audio)	111
□ multimedia (other)	95
□ multimedia (TV/video)	383

Selected Applications and Filters (2)

- Categories: instant messaging, social networking
- Categories: social networking

记录日志到FMC



Add Rule

Name: Block_Social and InstantMessag ☑ Enabled Insert: below rule 5

Action: Block

☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

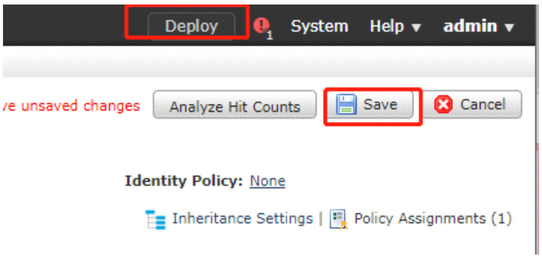
□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides

□ SNMP Trap Select an SNMP Alert Configuration...



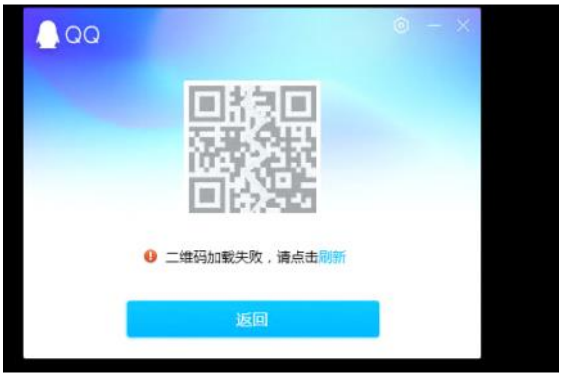
ve unsaved changes

Identity Policy: None

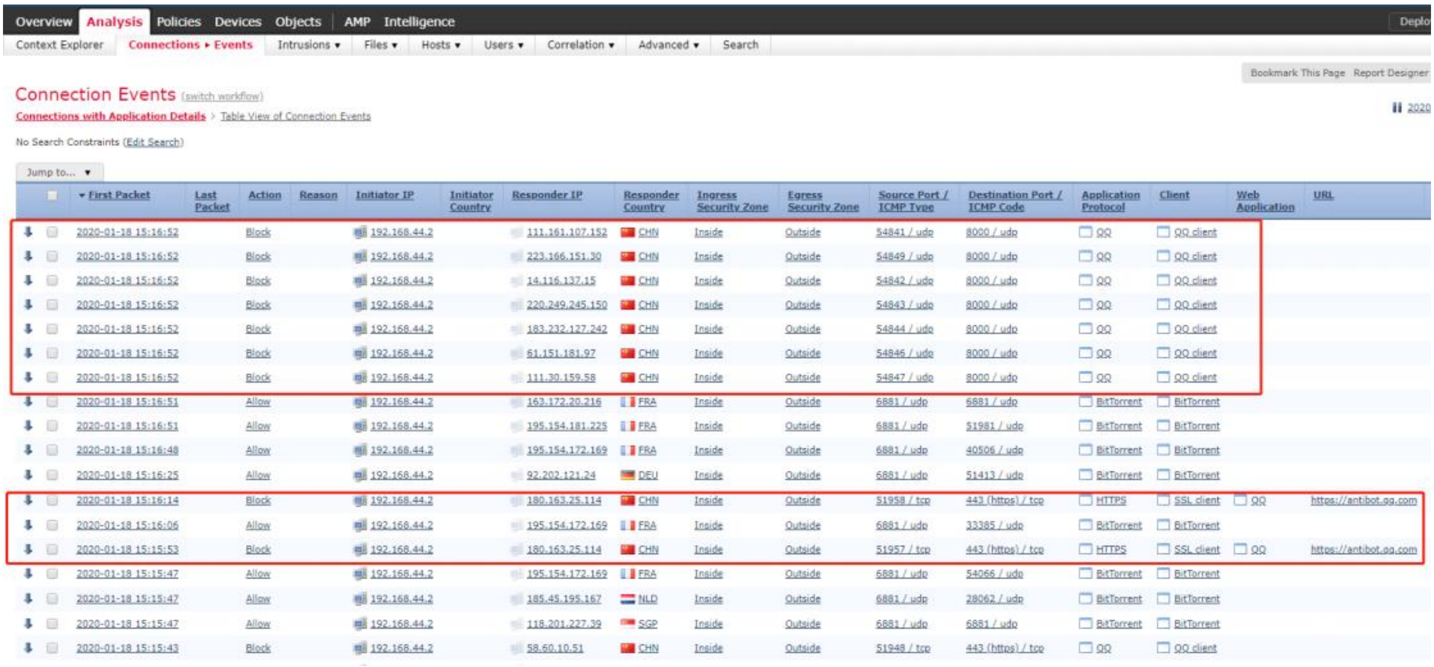
Inheritance Settings | Policy Assignments (1)

5.2：验证

登陆都无法登陆。



二维码加载失败，请点击刷新



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL
☐	2020-01-18 15:16:52		Block		192.168.44.2		111.161.107.152	CHN	Inside	Outside	54841 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		223.166.151.30	CHN	Inside	Outside	54849 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		14.116.137.15	CHN	Inside	Outside	54842 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		220.249.245.150	CHN	Inside	Outside	54843 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		183.232.127.242	CHN	Inside	Outside	54844 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		61.151.181.97	CHN	Inside	Outside	54846 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:52		Block		192.168.44.2		111.30.159.58	CHN	Inside	Outside	54847 / udp	8000 / udp	QQ	QQ client		
☐	2020-01-18 15:16:51		Allow		192.168.44.2		163.172.20.216	FRA	Inside	Outside	6881 / udp	6881 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:16:51		Allow		192.168.44.2		195.154.181.225	FRA	Inside	Outside	6881 / udp	51981 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:16:48		Allow		192.168.44.2		195.154.172.169	FRA	Inside	Outside	6881 / udp	40506 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:16:25		Allow		192.168.44.2		92.202.121.24	DEU	Inside	Outside	6881 / udp	51413 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:16:14		Block		192.168.44.2		180.163.25.114	CHN	Inside	Outside	51958 / tcp	443 (https) / tcp	HTTPS	SSL client	QQ	https://antibot.qq.com
☐	2020-01-18 15:16:06		Allow		192.168.44.2		195.154.172.169	FRA	Inside	Outside	6881 / udp	33385 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:15:53		Block		192.168.44.2		180.163.25.114	CHN	Inside	Outside	51957 / tcp	443 (https) / tcp	HTTPS	SSL client	QQ	https://antibot.qq.com
☐	2020-01-18 15:15:47		Allow		192.168.44.2		195.154.172.169	FRA	Inside	Outside	6881 / udp	54066 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:15:47		Allow		192.168.44.2		185.45.195.167	NLD	Inside	Outside	6881 / udp	28062 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:15:47		Allow		192.168.44.2		118.201.227.39	SGP	Inside	Outside	6881 / udp	6881 / udp	BitTorrent	BitTorrent		
☐	2020-01-18 15:15:43		Block		192.168.44.2		58.60.10.51	CHN	Inside	Outside	51948 / tcp	443 (https) / tcp	QQ	QQ client		

5.3：TroubleShooting

```
> system support firewall-engine-debug        //FTD查看debug防火墙引擎的实时调试信息
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
```

```
> system support application-identification-debug    //FTD 查看应用标识编号的调试信息
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:

Monitoring application identification debug messages . .
172.16.100.110-4677 -> 31.13.65.36-443 6 R AS 4 I 1 port service 0
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 3rd party returned 847
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 SSL is service 1122,
portServiceAppId 1122
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 ssl returned 10
172.16.100.110-4677 -> 31.13.65.36-443 6 AS 4 I 1 appId: 629
(safe)search_support_type=NOT_A_SEARCH_ENGINE ^C
Caught interrupt signal
```

```
admin@FMC:~$ sudo OmniQuery.pl -db mdb -e "select appId,appName from appIdInfo where appId=629"; //FMC查看应用标识是不是该应用
Password:
getting filenames from [/usr/local/sf/etc/db_updates/index]
getting filenames from [/usr/local/sf/etc/db_updates/base-6.1.0]
+-------+----------+
| appId | appName |
+-------+----------+
| 629 | Facebook |
+-------+----------+
```