

Interop Tokyo 2015 ShowNetにおける BGP Flowspec相互接続検証

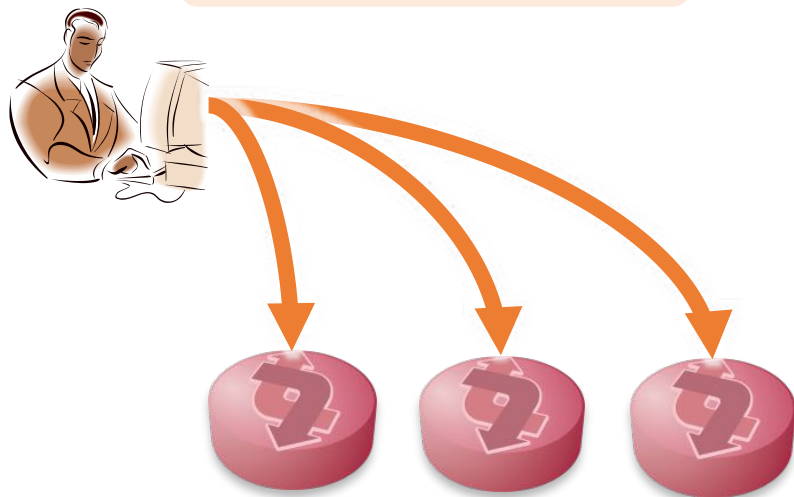
ShowNet NOCチームメンバー
大久保 修一



BGP Flowspec(RFC5575)

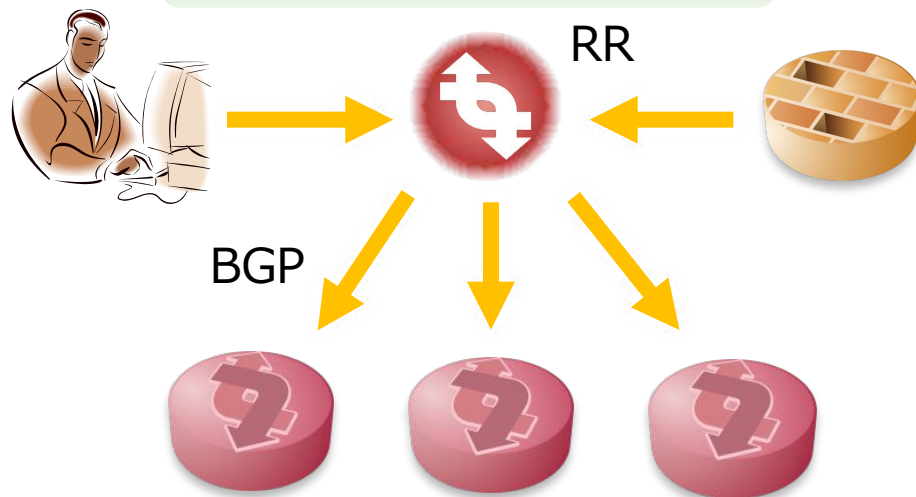
- BGPでACL設定を網内のルータ群に配布するイメージ

従来のACL設定は



1台1台設定が大変・・・

BGP Flowspecを使用

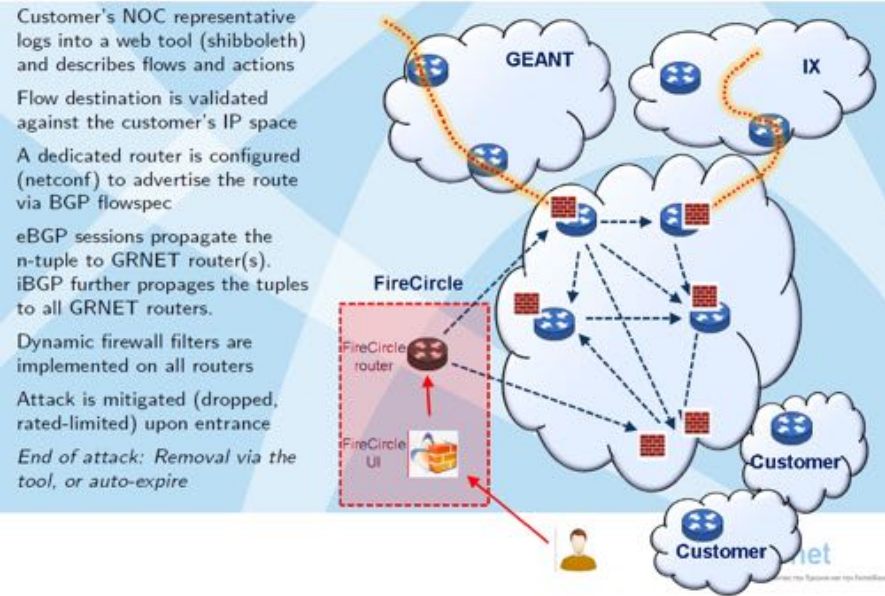


セキュリティアプライアンスとの連携も容易

日本国外での導入事例

GRNETの例

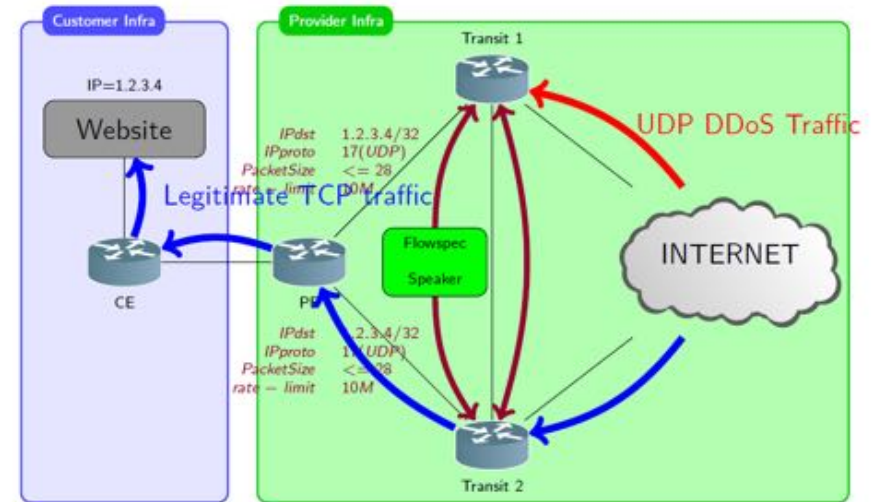
FireCircle Operation Overview



<https://tnc2012.terena.org/core/presentation/41>

NEO TELECOMSの例

Real life architecture



http://media.frnog.org/FRnOG_18/FRnOG_18-6.pdf

日本国外での導入事例

GRNETの例

FireCircle Operation Overview

Customer's NOC representative logs into a web tool (shibboleth) and describes flows and actions

Flow destination is validated against the customer's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s). iBGP further propagates the tuples to all GRNET routers.

Dynamic firewall filters are implemented on all routers

Attack is mitigated (dropped, rate-limited) upon entrance

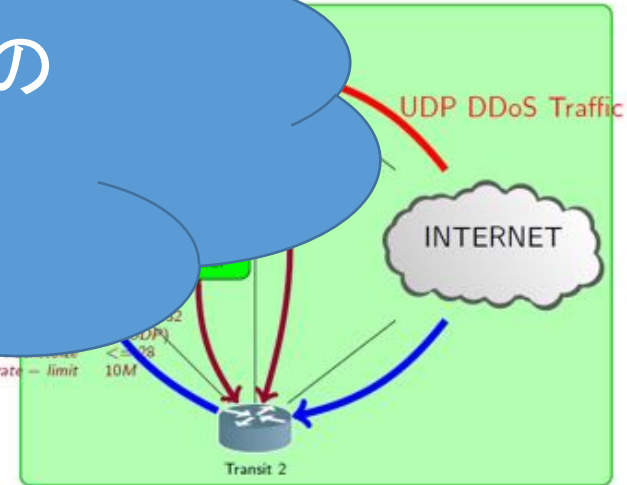
End of attack: Removal via the tool, or auto-expire



NEO TELECOMSの例

Real life architecture

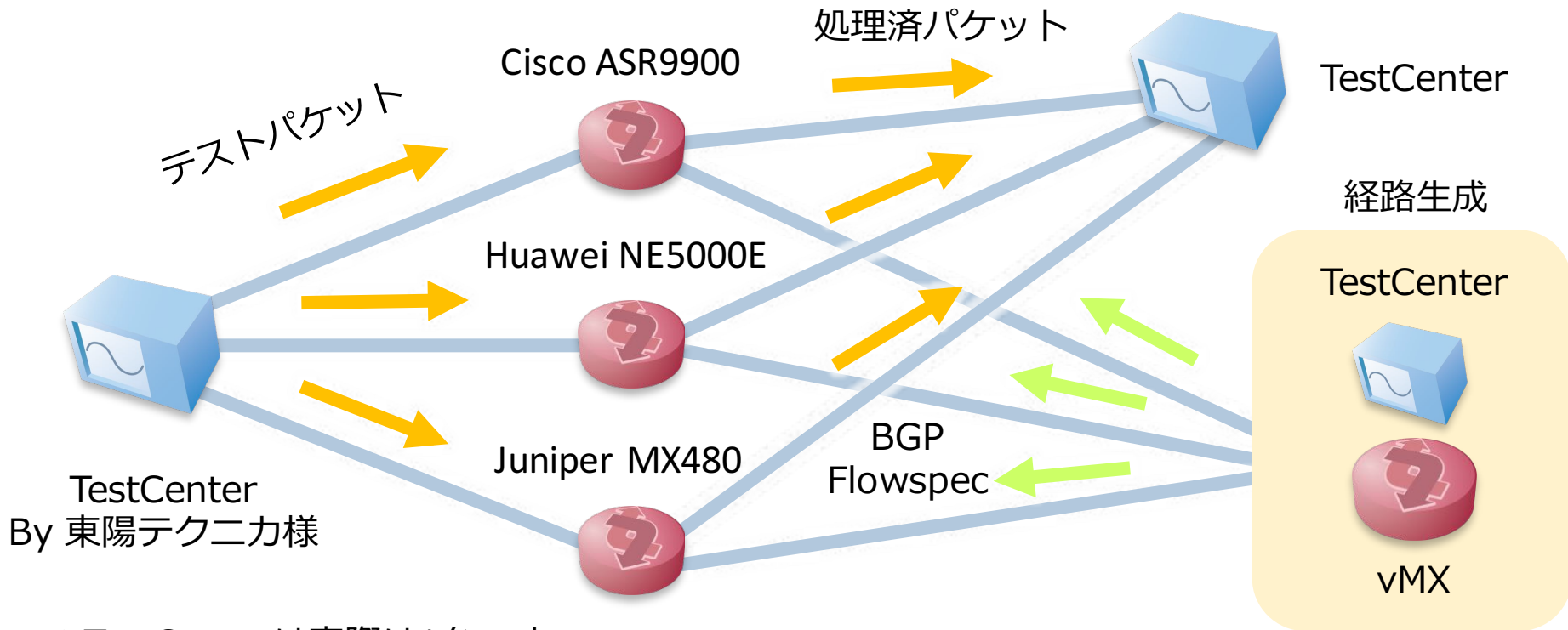
ただし、マルチベンダでの
相互接続検証事例は、
あまりなさそう



<https://tnc2012.terena.org/core/presentation/41>

http://media.frnog.org/FRnOG_18/FRnOG_18-6.pdf

ShowNetでの相互接続検証構成



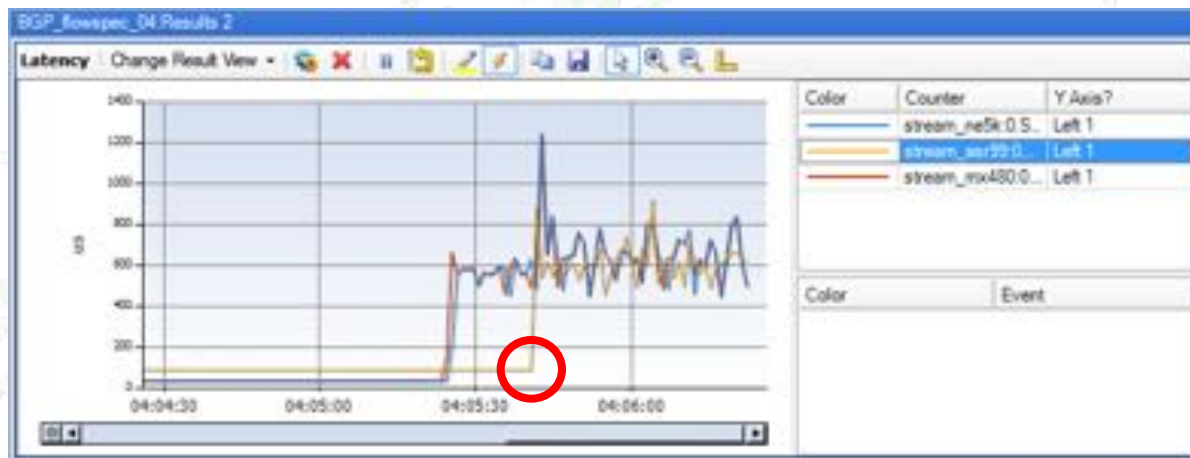
※ TestCenterは実際は1台です。

アクション指定によるテスト結果

テスト項目	NE5000E	ASR9900	MX480
Drop (パケット破棄)	○	○	○
Rate-limit (帯域制限)	○	○	○
VRF Redirect	○	○	○

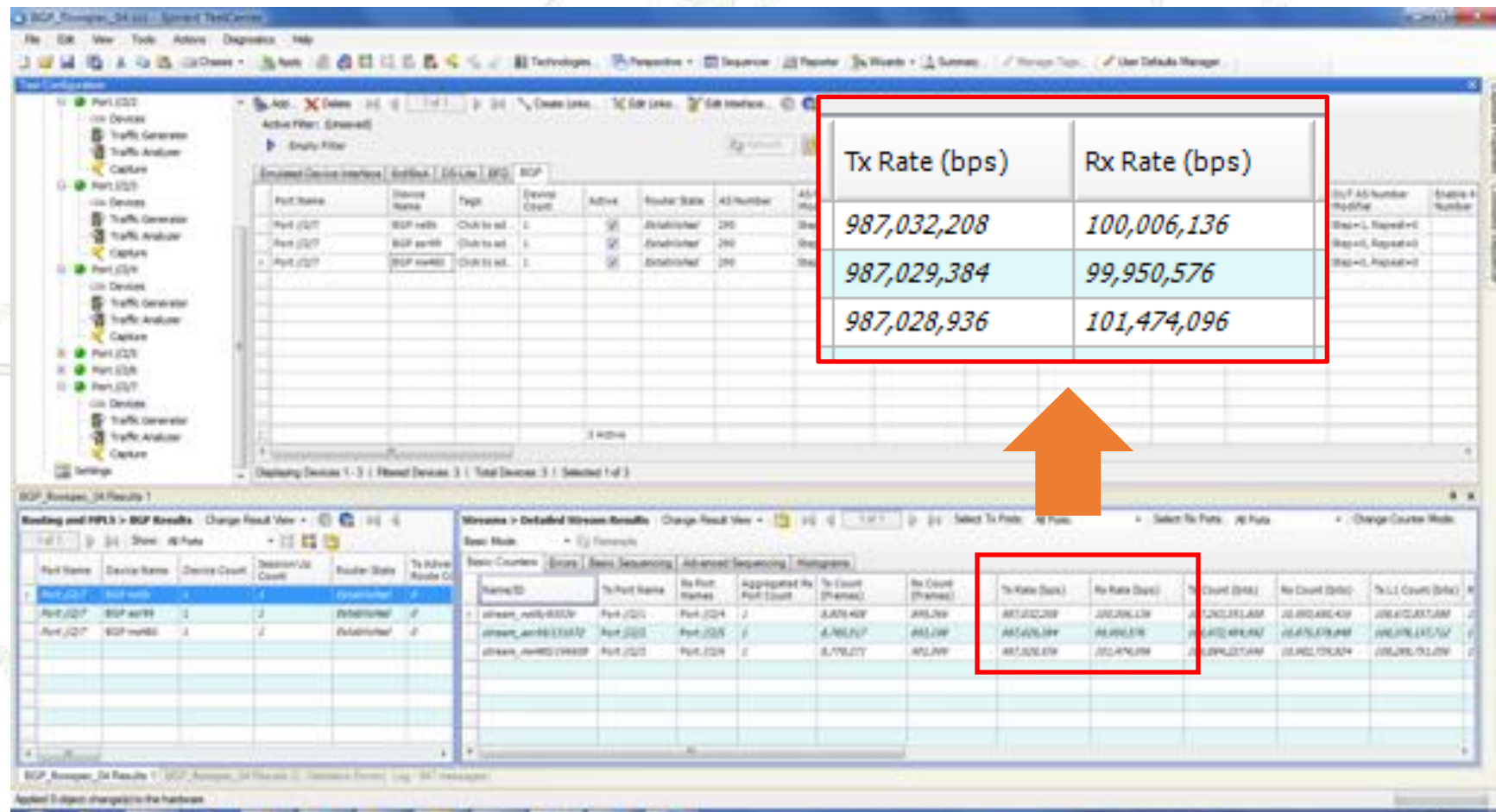
- DropアクションはRate-limit=0の設定
- Rate-limitは、100Mbpsに制限する経路情報を注入し、TestCenterから1Gbpsのトラフィックを送信し、受信レートを測定することで確認
- Redirectは、3ルータのインターフェイスカウンタ、およびTestCenterでの受信トラフィックレイテンシ測定により確認

レイテンシ



- Redirect後の通信経路上、レイテンシが変化することで確認（ルータのForwarding性能劣化ではない）
- ASR9900において、Redirectアクションを行う経路情報を注入後、転送処理に反映されるまで10秒前後かかる挙動が確認された。Withdrawnの場合は即座に反映される。
- BGPのNext-hop Scan Timerに依存しており、チューニング可能とのこと

Rate-limit



タイプごとの動作テスト結果

テスト項目	NE5000E	ASR9900	MX480
Type 1 - Destination Prefix	○	○	○
Type 2 - Source Prefix	○	○	○
Type 3 - IP Protocol	○	○	○
Type 4 - Port	—	—	—
Type 5 - Destination port	○	○	○
Type 6 - Source port	○	○	○
Type 7 - ICMP type	○	○	○
Type 8 - ICMP code	○	○	○
Type 9 - TCP flags	○ (NLRIの違いあり)	○ (NLRIの違いあり)	○
Type 10 - Packet length	次期バージョンで対応予定	○	○
Type 11 - DSCP	○	○	○
Type 12 - Fragment	— (NLRIの違いあり)	○	○

Type9. TCP FlagsのNLRIの違い

Juniper

syn+ackを設定した場合

Dest	/32	45.0.2.54	Src	/32	45.0.2.42	TCP Flg.	op	Bit mask	op	Bit mask
0x01	202d0002	3602	202d0002	22a0	9000	0280	10			

0x02 SYN

0x10 ACK

Cisco

Dest	/32	45.0.2.54	Src	/32	45.0.2.42	TCP Flg.	op	Bit mask
0x01	202d0002	3602	202d0002	22a0	9811	12		

0x12
ACK-SYN

Type9. TCP FlagsのNLRIの違い

ASR側で経路受信するも
想定した動作にならず



Interop期間中に、シスコ様にて
スペシャルファームを作成いただき、
想定動作になることを確認

Type9. Type12. マッチビットの違い

Juniper

op=0x80

0	1	2	3	4	5	6	7							
+	-	+	-	+	-	+	-							
+	-	+	-	+	-	+	-							
	e		a		len		0		0		not		m	
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+
1	0	0	0	0	0	0	0	0						

Cisco, Huawei

op=0x81

0	1	2	3	4	5	6	7							
+	-	+	-	+	-	+	-							
+	-	+	-	+	-	+	-							
	e		a		len		0		0		not		m	
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+
1	0	0	0	0	0	0	0	1						

m=0の場合、NE5000Eが
Invalid判定してしまう



ファアーウェイ様より、
将来的に対応予定とのこと
(m=0も受信するように)

ShowNetでの運用例

ShowNetバックボーン機器への
SSHブルートフォース攻撃が常時発生



BGP Flowspecを用いてフィルタリングを実施

1. 踏み台サーバのTCP 22番ポートは許可
2. 45.0.0.0/16 TCP 22番,23番ポート宛てをDrop

評価順序が重要に

JUNOSの場合、以下の設定が必要

```
set routing-options flow term-order standard
```

http://www.juniper.net/documentation/en_US/junos14.2/topics/topic-map/bgp-flow-routes.html

By default, the Junos OS uses the term-ordering algorithm defined in version 6 of the BGP flow specification draft. In Junos OS Release 10.0 and later, you can configure the router to comply with the term-ordering algorithm first defined in version 7 of the BGP flow specification and supported through RFC 5575, Dissemination of Flow Specification Routes.

Best Practice: We recommend that you configure the Junos OS to use the term-ordering algorithm first defined in version 7 of the BGP flow specification draft. We also recommend that you configure the Junos OS to use the same term-ordering algorithm on all routing instances configured on a router.

SAMURAIとの連携デモ

正常通信

DDoS緩和装置

④ 攻撃のみを除去し、
正常通信は戻す

Cisco ASR9900

Huawei NE5000E

③ VRF
リダイレクト

Juniper MX480

トラフィック情報
(xFlow)

Webサーバ
(victim)

Route-Reflector

Juniper vMX

② flowspec
経路広告

① 攻撃検知

DDoS攻撃

DDoS攻撃

疑似攻撃者

BOTへの指示

BOTへの指示



Attack ID	Source	Destination	Protocol	Port	Count	Time	Status
101	192.168.1.1	192.168.1.1	TCP	80	1000	2015-01-01 10:00:00	Active
102	192.168.1.2	192.168.1.1	TCP	80	500	2015-01-01 10:00:00	Active
103	192.168.1.3	192.168.1.1	TCP	80	200	2015-01-01 10:00:00	Active
104	192.168.1.4	192.168.1.1	TCP	80	100	2015-01-01 10:00:00	Active
105	192.168.1.5	192.168.1.1	TCP	80	50	2015-01-01 10:00:00	Active
106	192.168.1.6	192.168.1.1	TCP	80	20	2015-01-01 10:00:00	Active
107	192.168.1.7	192.168.1.1	TCP	80	10	2015-01-01 10:00:00	Active
108	192.168.1.8	192.168.1.1	TCP	80	5	2015-01-01 10:00:00	Active
109	192.168.1.9	192.168.1.1	TCP	80	2	2015-01-01 10:00:00	Active
110	192.168.1.10	192.168.1.1	TCP	80	1	2015-01-01 10:00:00	Active

Special Thanks

多大なるご協力を賜り誠にありがとうございました

