FDNet: Инструмент для формального описания сетей v1.1

Vasily A. Sartakov

21 октября 2014 г.

1 Введение

fdnet представляет собой набор утилит и онтологий позволяющих описывать сети в машино-интерпретируемом формате.

2 Формат представления данных

Данные представлены в формате Resource Description Framework (RDF) [2]. RDF является одним из инструментов семантического веба для представления связанных сущностей. Сущности представлены в форме «субъект-предикат-объект».

В текущей версии мы используем нотацию RDF n3[1], преобразуя ее в формат RDF XML при помощи утилиты *cwm*. Пример:

```
@forSome <#unit_id> .
<#unit_id>              a                       <Unit_Desc> .
<#unit_id>              <name>                  "Name of entity" .
<#unit_id>              <feature>               "555-55-45" .
<#unit_id>              <predicat>              <#another_id> .
```

В примере объявляется сущность класса «Unit_Desc» идентифицируема через #unit_id. Эта сущность имеет три свойства: поле *name* с значением «Name of entity», поле *feature* с значением «Name of entity», и свойство *predicat*, указывающее на другую сущность идентифицируемое через #another_id. Каждая строка в описании заканчивается точкой. Класс (тип) сущности определяется через предикат *a*

Важно: Имена и идентификаторы всех сущностей должны быть уникальными в пределах одной сети.

3 Онтология

В настоящий момент для представления конфигурации сети разработаны несколько классов. Каждый из классов описывает каку-то определенную

сущность и ее характеристики. Описание классов производится в формате RDF Schema в формате XML. Данный момент существуют следующие классы:

- Rack
- Unit
- Switch
- Port
- NetDev
- Subnet
- Server
- Model
- Program

3.1 Rack

Сущность *Rack* описывает серверную стойку.

name
Имя, название, идентификатор стойки.

sn
Серийный номер. Уникальный идентификатор.

maxUnits
Максимальное количество юнитов в стойке.

hasUnit
Специальный предикат указывающий на сущность Unit, занимающую место в этой стойке.

Пример

```
@forSome <#rack1> .
<#rack1>                a <Rack> .
<#rack1>                <name>                  "rack" .
<#rack1>                <sn>                    "555-55-45" .
<#rack1>                <maxUnits>              "25" .
<#rack1>                <hasUnit>               <#r1_u0> .
...
<#rack1>                <hasUnit>               <#r1_u24> .
```

В примере объявляется стойка идентифицируемая по #rack1. Стойка называется «rack», с серийным номером 555-55-45 и количеством юнитов в 25. Так же эта стойка заполнена сущностями unit идентифицируемые с #r1_u0 до #r1_u24.

3.2 Unit

Сущность *Unit* описывает размещение какого-то устройства в стойке.

number
Номер этого юнита в стойке.

occupiedBy
В логическом Unit располагается одной устройство, и сущность *occupiedBy* указывает на это устройство.

Пример

```
@forSome <#r1_u11> .
<#r1_u11>               a                       <Unit> .
<#r1_u11>               <number>                "11" .
<#r1_u11>               <occupiedBy>            <#Switch2> .

@forSome <#r1_u12> .
<#r1_u12>               a                       <Unit> .
<#r1_u12>               <number>                "12" .
<#r1_u12>               <occupiedBy>            <#APMS> .
```

В данном примере представлены два юнита идентифицируемые через #r1_u11 и #r1_u12. Эти сущности описывают юниты 11 и 12 соответственно. В первом случае этот юнит занят оборудованием идентифицируемом через #Switch2, а во втором - #APMS

3.3 Switch

Сущность *Switch* описывает сетевой коммутатор.

name
Коммутатор обладает свойством имени.

sn
Коммутатор обладает уникальным идентификатором.

model
Сетевой коммутатор имеет физические характеристики и эти характеристики описаны в моделе.

mngPort
В коммутаторе может присутствовать сконфигурированный порт управления.

port
В коммутаторе может присутствовать сетевой порт и эта сущность на него ссылается.

ip
У коммутатора может быть свой собственный IP адрес.

```
@forSome <#Switch2> .
<#Switch2>              a                       <Switch> .
<#Switch2>              <name>                  "Switch2" .
<#Switch2>              <sn>                    "111-456" .
<#Switch2>              <model>                 <#CISCO2950> .
<#Switch2>              <mngPort>               "0" .
<#Switch2>              <port>                  <#sw2_p1> .
<#Switch2>              <port>                  <#sw2_p2> .
```

В примере объявляется коммутатор идентифицируемый через #Switch2. У этого устройства есть имя - «Switch2», серийный номер 111-456, два порта идентифицируемые через #sw2_p1 и #sw2_2, а так же указан тип модели, идентифицируемые через #CISCO2950

3.4 Port

Сущность порт описывает физический порт на коммутаторе.

number
У порта есть основное свойство - его номер.

type
Тип порта: UTP, оптика.

speed
Скорость: 10/100/1000Mbps

connectedWith
Какое устройство подсоединено к этому порту.

Пример

```
@forSome <#sw1_p2> .
<#sw1_p2>               a                       <Port> .
<#sw1_p2>               <number>                "2" .
<#sw1_p2>               <speed>                 "1Gb" .
<#sw1_p2>               <type>                  "UTP" .
<#sw1_p2>               <connectedWith>         <#S3_eth0> .
```

В этом примере #sw1_p2 является идентификатором порта. #S3_eth0 - идентификатор сетевого устройства подключенного к этому порту.

3.5 NetDev

Сетевое устройствой NetDev является физической сущностью описывающей реальное физическое устройство. Через это устройство осуществляется подключение сервера к сетевому оборудованию или другим серверам.

name
Имя сетевого устройства в системе.

type
Тип подключения

speed
Скорость сетевого устройства

hwAddr
Аппаратный адрес hwAddr является обязательным описанием устройства NetDev, без него невозможно построить правило для IP <-> MAC

ip
IP адрес является свойством сущностью NetDev и привязан к конкретному сетевому устройству.

connectedWith
Сетевое устройство коммутируется с другими сетевыми устройствами или портами на сетевом оборудовании

Пример

```
@forSome <#S3_eth0> .
<#S3_eth0>      a <NetDev> .
<#S3_eth0>      <name>          "eth0" .
<#S3_eth0>      <ip>            "2.4.1.1" .
<#S3_eth0>      <hwAddr>        "00-00-02-04-01-01" .
<#S3_eth0>      <speed>         "1Gb" .
<#S3_eth0>      <type>          "UTP" .
<#S3_eth0>      <connectedWith> <#sw1_p2> .
```

В данном примере описано сетевое устройство идентифицируемое через #S3_eth0. Это устройство присутствует в системе под именем «eth0», имеет IP адрес «2.4.1.1», MAC адрес «00-00-02-04-01-01», подключение осуществляется через витую пару UTP и скорость устройства 1Gb. Это сетевое устройство скомутировано с портом идентифицируемым через #sw1_p2.

3.6 Subnet

Подсеть является логической сущностью объединяющая в себе один или несколько логических серверов. В любой цифровой сети должна пресутствовать хотя бы одна логическая подсеть.

name
Сущеность *Subnet* обладает свойством имени.

hasServer
В подсеть могут входить сервера.

Пример

```
@forSome <#net1> .
<#net1>          a               <Subnet> .
<#net1>          <name>          "NET1" .
<#net1>          <hasServer>     <#SPS> .
<#net1>          <hasServer>     <#APMS> .

@forSome <#net2> .
<#net2>          a <Subnet> .
<#net2>          <name>          "NET2" .
<#net2>          <hasServer>     <#SS> .
```

В примере объявлены две подсети. Первая идентифицируется при помощи #net1, вторая - #net2. Первая подсеть имеет имя «NET1» и в ней присутствуют два сервера идентифицируемые через #SPS и #APMS. Вторая подсеть имеет имя «NET2» и в ней присутствует сервер идентифицируемые через #SS.

3.7 Server

Сущность *Server* является важной сущностью в цифровой сети. Во-первых, сервер является одновременно физической и логической сущность. Физической, так как сервер размещается в юнитах, которые находся в стойках. Физический сервер описан при помощи модели, содержащей физические характеристики (см. 3.8). В тоже время, логический сервер является частью логической подсети, в нем исполняются логические программы, коммуницирующие с другими сетевыми программами. Во вторых, правила сетевой безопасности описываются на основе сетевых адресов привязанных к конкретным серверам. В тоже время, правила контролируют поведение трафика, источником которых являются программы, исполняющиеся внутри логических серверов. В третьих, для уменьшения сложности цифровой сети, сервер может выступать в качестве реплики какого-то другого сервера. В этом случае он полностью повторяет функционал реплецируемого сервера, но не содержит собственного.

name
У сервера есть свойство имени. Он дожен быть назван.

hasDevice
У сервера есть сетевое устройство.

model
Сервер обладает физическими характеристиками, описанными в виде модели.

hasProgram
На логическим сервере могут исполняться программы.

replica
Сервер может быть репликой какого-то другого сервера.

ip
В исключительные ситуациях, при описании группы серверов выступающих в роли реплик и при отсутствии формального их описания (конкретных IP и MAC, подключение и прочего) эта группа сервером может быть описана через маску в этом поле. Для однозначно формализуемых сервером необходимо использовать NetDev

description
Поле с описанием (любыми комментариями) о сервере.

Пример

```
@forSome <#SS> .
<#SS>           a               <Server> .
<#SS>           <name>          "SS" .
<#SS>           <hasDevice>     <#SS_eth0> .
<#SS>           <model>         <#simple1U> .
<#SS>           <hasProgram>    <#ss_sps_1414> .

@forSome <#S2> .
<#S2>           a               <Server> .
<#S2>           <name>          "S2" .
<#S2>           <hasDevice>     <#S2_eth0> .
<#S2>           <model>         <#simple1U> .
<#S2>           <replica>       <#SS> .

@forSome <#APM4> .
<#APM4>         a <Server> .
<#APM4>         <name>          "APM4" .
<#APM4>         <replica>       <#APMS> .
<#APM4>         <ip>            "192.168.0.0/24" .
```

В данном примере объявляются два сервера идентифицируемые соответственно через #SS и #S2 и группа сервером #APM4. Первый сервер называется «SS», имеет сетевое устройство индентифицируемое через #SS_eth0, построен на основе модели идентифицируемой через #simple1U, а так же внутри сервера исполняется программа идентифицируемая через #ss_sps_1414. Второй сервер называется «S2», он имеет сетевое устройство идентифицируемое через #S2_eth0, он так же построен на основе модели #simple1U. В отличие от сервера #SS, второй сервер является репликой сервера идентифицируемого через #SS, а значит на нем нет собственных сервисов.

Группа серверов идентифицируемая как #APM4 является репликой сервера идентифицируемого через #APMS, при этом мы не можем указать ни размещение этих серверов, ни модели, ни подключение. Но, мы можем указать диапазон IP адресов входящих в эту группу, а так же ссослаться на сервер, который эта группа реплицирует.

3.8 Model

Model является логической сущностью описывающей физические характеристики сетевого оборудования.

name
Модель устройства, имя.

size
Высота устройства в юнитах.

power
Потребляемая мощность, в Ваттах.

cooling
Требования по охлаждению, BTU/hr (британская термическая единица в час)

weight
Масса устройства в килограммах.

Пример

```
@forSome <#CISCO2950> .
<#CISCO2950>            a               <Model> .
<#CISCO2950>            <name>          "Cisco Catalyst 2950-24" .
<#CISCO2950>            <size>          "1U" .
<#CISCO2950>            <power>         "30" .
<#CISCO2950>            <cooling>       "nan" .
<#CISCO2950>            <weight>        "3" .
```

В данном примере описано сетевое оборудование Cisco Catalust 2950-24 идентифицируемое через #CISCO2950. Этот тип оборудования имеет название, оно занимает 1U, требует 30Ват мощности, имеет массу в 3 кг и по нему отсетствует информация о требованиях к охлаждению.

3.9 Program

Program является ключевой сущностью при описании взаимодействия. Именно программы могут коммуницировать друг с другом.

name
У программы есть имя.

listenPort

Программа может открывать порт и «слушать» обращения к нему. Программа выступает в роли программы-сервера.

communicateWith

Программа может взаимодействовать с другими программами. В этом случае взаимодействие с программой указывается через предикат *communicateWith*

Пример

```
@forSome <#sps_mysql_3306> .
<#sps_mysql_3306>       a                       <Program> .
<#sps_mysql_3306>       <name>                  "mysql" .
<#sps_mysql_3306>       <listenPort>            "3306" .
<#sps_mysql_3306>       <communicateWith>       <#sps_mysql_3306> .

@forSome <#sps_crypto_80> .
<#sps_crypto_80>        a <Program> .
<#sps_crypto_80>        <name>          "crypto_server1" .
<#sps_crypto_80>        <listenPort>    "80" .

@forSome <#apms_sps_80> .
<#apms_sps_80>  a                       <Program> .
<#apms_sps_80>  <name>                  "crypto_client" .
<#apms_sps_80>  <communicateWith>       <#sps_crypto_80> .
```

В примере представлены 3 программы. Первая из них идентифицируема через #sps_mysql_3306 называется «mysql». У этой программы открыт порт 80, при этом она сама может коммуницировать с программой идентифицируемой через #sps_mysq_3306, т.е. с самой собой. Это значит, например, что программа #sps_mysql_3306 может исполняться на нескольких реплицируемых машинах выполняя при этом операции репликации базы данных.

Вторая программа идентифицируется через #sps_crypto_80. Она называется «crypto_server 1» и выступает в роли программы-сервера открывая порт 80.

Третья программа идентифицируемая через #apms_sps_80 имеет называние «crypto_client» и выступает в роли программы-клиента коммуницируя с программой идентифицируемой через #sps_crypto_80.

Важно заметить, что все три программы могут исполняться внутри реплицируемых серверов.

4 fdnet.py

Скрипт *fdnet.py* формирует набор SNORT правил на основе формально описанной сети. Необходимым аргументом этого скрипта является путь до описания сети в формате rdf/xml и комманда скрипту. rdf/xml может быть получен из n3 используя утилиту *cwm*:

```
cwm -n3 net.n3 -rdf=b >net.rdf
python fdnet.py --database net.rdf all
```

4.1 Комманды

Скрипт выполняет следующие комманды:

- all выполняет все комманды последовательно
- diag создает только диаграмму взаимодействия програм
- rules создает только список правил
- plan формирует IP план
- conn формирует список подключений
- place формирует описание физического размешения оборудования

4.2 Выходные данные

Скрипт на выходе скрипт создает несколько файлов:

- sid-msg.map Набор идентифицаторов и сообщений о вторжении. Каждый номер (sid) используется в описании правила для SNORT/Suricata. Номера уникальны в рамках одной сети.
- net.dot Исходный файл схемы, на основе которого создается файл .png
- net.png Наглядное представление структуры сети с точки зрения взаимодействующих компонент (программ), их аффилиация с серверами (и репликами), а так же размещение логических серверов внутри логических сетей.
- net.rules Файл содержащий правила для SNORT/Suricata
- net_ip-plan.xlsx Таблица описывающая структуру сети с точки зрения назначения IP адресов оборудованию
- net_phys.xlsx Таблица описывающая физическое размещение оборудования в серверной комнате
- net_place.xlsx Таблица описывающая размещение и коммутиацию оборудоания

4.3 Требования к описанию сети

Минимальными требованиями для создания SNORT/Suricata правил следующие:

- Subnet
  - name

  - hasServer

- Server
  - name
  - hasDevice
  - hasProgram

- NetDev
  - ip
  - hwAddr
  - connectedWith

- Program
  - name
  - listenPort
  - communicateWith

При этом, скрипт корректно отработает, если в цифровой сети будут присутствовать сервера без программ. Скрипт сможет корректно отрабать, если в сети не будет Subnet, если в сети будет находится ни с кем не взаимодействующая программа, или у сервера не будет указан IP или имя.

Для создания описания физической конфигурации необходимо указать следующий минимальный набор объектов:

- Rack
  - hasUnit
  - name

- Unit
  - occupiedBy
  - number

- Server
  - name
  - connectedWith
  - hasDevice
  - model

- NetDev
  - ip
  - connectedWith

- Model
  - name

  - power
  - size
  - weight
  - cooling
- Port
  - name
  - number
  - connectedWith

4.4 TODO

Хотелось бы доработать следующие моменты:

- Нужна валидация цифровой сети по схеме
- Нужно проверить корректность работы с множеством сетевых адресов и подключений
- Нужно описать пример

5 Пример

TBD...

В приложении представлена тестовая схема сети. В ней использован следующий подход при выборе имен и идентификаторов:

- –

Список литературы

[1] Rdf notation3. `http://en.wikipedia.org/wiki/Notation3`.

[2] Graham Klyne and Jeremy J Carroll. Resource description framework (rdf): Concepts and abstract syntax. 2006.

Listing 1: Тестовая схема сети

```
#
# clients
#

#sp1

@forSome <#sps_css_10060> .
<#sps_css_10060> a <Program> .
<#sps_css_10060> <name>   "client 10060" .
<#sps_css_10060> <communicateWith> <#css_srv_10060> .

#apm

@forSome <#apms_sps_80> .
<#apms_sps_80> a <Program> .
<#apms_sps_80> <name>   "apms to sp1 crypto 80" .
<#apms_sps_80> <communicateWith> <#sps_crypto_80> .

@forSome <#apms_sps_8000> .
<#apms_sps_8000> a <Program> .
<#apms_sps_8000> <name>   "apms to sp1 crypto 8000" .
<#apms_sps_8000> <communicateWith> <#sps_crypto_8000> .

@forSome <#apms_vpns_666> .
<#apms_vpns_666> a <Program> .
<#apms_vpns_666> <name>   "apms tp vpn client" .
<#apms_vpns_666> <communicateWith> <#vpns_vpn_666> .

@forSome <#apms_css_666> .
<#apms_css_666> a <Program> .
<#apms_css_666> <name>   "apms to cs vpn client" .
<#apms_css_666> <communicateWith> <#css_vpn_666> .

#X

@forSome <#x_vpns_666> .
<#x_vpns_666> a <Program> .
<#x_vpns_666> <name>   "x vpns client" .
<#x_vpns_666> <communicateWith> <#vpns_vpn_666> .

@forSome <#x_css_666> .
<#x_css_666> a <Program> .
<#x_css_666> <name>   "x vpn client" .
<#x_css_666> <communicateWith> <#css_vpn_666> .

@forSome <#x_sps_22> .
<#x_sps_22> a <Program> .
<#x_sps_22> <name>   "ssh client" .
```

<#x_sps_22> <communicateWith> <#sps_sshd_22> .

@forSome <#x_sps_199> .
<#x_sps_199> a <Program> .
<#x_sps_199> <name> "199 client" .
<#x_sps_199> <communicateWith> <#sps_199_199> .

@forSome <#x_sps_514> .
<#x_sps_514> a <Program> .
<#x_sps_514> <name> "514 client" .
<#x_sps_514> <communicateWith> <#sps_514_514> .

#S

@forSome <#ss_sps_1414> .
<#ss_sps_1414> a <Program> .
<#ss_sps_1414> <name> "ss vpn" .
<#ss_sps_1414> <communicateWith> <#sps_vpn_1414> .

#
program servers
#

sps

@forSome <#sps_mysql_3306> .
<#sps_mysql_3306> a <Program> .
<#sps_mysql_3306> <name> "mysql" .
<#sps_mysql_3306> <listenPort> "3306" .
<#sps_mysql_3306> <communicateWith> <#sps_mysql_3306> .

@forSome <#sps_crypto_80> .
<#sps_crypto_80> a <Program> .
<#sps_crypto_80> <name> "crypto_server1" .
<#sps_crypto_80> <listenPort> "80" .

@forSome <#sps_crypto_8000> .
<#sps_crypto_8000> a <Program> .
<#sps_crypto_8000> <name> "crypto_server2" .
<#sps_crypto_8000> <listenPort> "8000" .

@forSome <#sps_sshd_22> .
<#sps_sshd_22> a <Program> .
<#sps_sshd_22> <name> "sshd" .
<#sps_sshd_22> <listenPort> "22" .

@forSome <#sps_199_199> .
<#sps_199_199> a <Program> .
<#sps_199_199> <name> "199 port" .

<#sps_199_199> <listenPort> "199" .

@forSome <#sps_514_514> .
<#sps_514_514> a <Program> .
<#sps_514_514> <name> "514 port" .
<#sps_514_514> <listenPort> "514" .

@forSome <#sps_vpn_1414> .
<#sps_vpn_1414> a <Program> .
<#sps_vpn_1414> <name> "1414 is open" .
<#sps_vpn_1414> <listenPort> "1414" .

css

@forSome <#css_vpn_666> .
<#css_vpn_666> a <Program> .
<#css_vpn_666> <name> "CFG_CS" .
<#css_vpn_666> <listenPort> "666" .

@forSome <#css_srv_10060> .
<#css_srv_10060> a <Program> .
<#css_srv_10060> <name> "10060 port" .
<#css_srv_10060> <listenPort> "10060" .

vpns

@forSome <#vpns_vpn_666> .
<#vpns_vpn_666> a <Program> .
<#vpns_vpn_666> <name> "VPN" .
<#vpns_vpn_666> <listenPort> "666" .

#devices

@forSome <#TOR_eth0> .
<#TOR_eth0> a <NetDev> .
<#TOR_eth0> <name> "eth0" .
<#TOR_eth0> <ip> "1.1.1.254" .
<#TOR_eth0> <hwAddr> "01−01−01−02−05−04" .
<#TOR_eth0> <speed> "1Gb" .
<#TOR_eth0> <type> "UTP" .
<#TOR_eth0> <connectedWith> <#sw2_p10> .

@forSome <#S3_eth0> .
<#S3_eth0> a <NetDev> .
<#S3_eth0> <name> "eth0" .
<#S3_eth0> <ip> "2.4.1.1" .
<#S3_eth0> <hwAddr> "00−00−02−04−01−01" .
<#S3_eth0> <speed> "1Gb" .
<#S3_eth0> <type> "UTP" .
<#S3_eth0> <connectedWith> <#sw1_p2> .

```
@forSome <#S2_eth0> .
<#S2_eth0>  a <NetDev> .
<#S2_eth0>  <name>  "eth0" .
<#S2_eth0>  <ip>  "2.3.1.1" .
<#S2_eth0>  <hwAddr> "00−00−02−03−01−01" .
<#S2_eth0>  <speed>  "1Gb" .
<#S2_eth0>  <type>  "UTP" .
<#S2_eth0>  <connectedWith> <#sw1_p3> .

@forSome <#SS_eth0> .
<#SS_eth0>  a <NetDev> .
<#SS_eth0>  <name>  "eth0" .
<#SS_eth0>  <ip>  "2.1.1.1" .
<#SS_eth0>  <hwAddr> "00−00−02−01−01−01" .
<#SS_eth0>  <speed>  "1Gb" .
<#SS_eth0>  <type>  "UTP" .
<#SS_eth0>  <connectedWith> <#sw1_p4> .

@forSome <#X_eth0> .
<#X_eth0>  a <NetDev> .
<#X_eth0>  <name>  "eth0" .
<#X_eth0>  <ip>  "3.1.1.1" .
<#X_eth0>  <hwAddr> "00−00−03−01−01−01" .
<#X_eth0>  <speed>  "1Gb" .
<#X_eth0>  <type>  "UTP" .
<#X_eth0>  <connectedWith> <#sw1_p1> .

@forSome <#APM3_eth0> .
<#APM3_eth0>  a <NetDev> .
<#APM3_eth0>  <name>  "eth0" .
<#APM3_eth0>  <ip>  "1.1.1.12" .
<#APM3_eth0>  <hwAddr> "00−00−01−01−01−12" .
<#APM3_eth0>  <speed>  "1Gb" .
<#APM3_eth0>  <type>  "UTP" .
<#APM3_eth0>  <connectedWith> <#sw2_p9> .

@forSome <#APM2_eth0> .
<#APM2_eth0>  a <NetDev> .
<#APM2_eth0>  <name>  "eth0" .
<#APM2_eth0>  <ip>  "1.1.1.11" .
<#APM2_eth0>  <hwAddr> "00−00−01−01−01−11" .
<#APM2_eth0>  <speed>  "1Gb" .
<#APM2_eth0>  <type>  "UTP" .
<#APM2_eth0>  <connectedWith> <#sw2_p8> .

@forSome <#APMS_eth0> .
<#APMS_eth0>  a <NetDev> .
<#APMS_eth0>  <name>  "eth0" .
<#APMS_eth0>  <ip>  "1.1.1.10" .
```

<#APMS_eth0> <hwAddr> "00−00−01−01−01−10" .
<#APMS_eth0> <speed> "1Gb" .
<#APMS_eth0> <type> "UTP" .
<#APMS_eth0> <connectedWith> <#sw2_p7> .

@forSome <#VPN2_eth0> .
<#VPN2_eth0> a <NetDev> .
<#VPN2_eth0> <name> "eth0" .
<#VPN2_eth0> <ip> "1.1.1.2" .
<#VPN2_eth0> <hwAddr> "00−00−01−01−01−02" .
<#VPN2_eth0> <speed> "1Gb" .
<#VPN2_eth0> <type> "UTP" .
<#VPN2_eth0> <connectedWith> <#sw2_p2> .

@forSome <#VPNS_eth0> .
<#VPNS_eth0> a <NetDev> .
<#VPNS_eth0> <name> "eth0" .
<#VPNS_eth0> <ip> "1.1.1.1" .
<#VPNS_eth0> <hwAddr> "00−00−01−01−01−01" .
<#VPNS_eth0> <speed> "1Gb" .
<#VPNS_eth0> <type> "UTP" .
<#VPNS_eth0> <connectedWith> <#sw2_p1> .

@forSome <#CS2_eth0> .
<#CS2_eth0> a <NetDev> .
<#CS2_eth0> <name> "eth0" .
<#CS2_eth0> <ip> "1.1.1.4" .
<#CS2_eth0> <hwAddr> "00−00−01−01−01−04" .
<#CS2_eth0> <speed> "1Gb" .
<#CS2_eth0> <type> "UTP" .
<#CS2_eth0> <connectedWith> <#sw2_p4> .

@forSome <#CSS_eth0> .
<#CSS_eth0> a <NetDev> .
<#CSS_eth0> <name> "eth0" .
<#CSS_eth0> <ip> "1.1.1.3" .
<#CSS_eth0> <hwAddr> "00−00−01−01−01−03" .
<#CSS_eth0> <speed> "1Gb" .
<#CSS_eth0> <type> "UTP" .
<#CSS_eth0> <connectedWith> <#sw2_p3> .

@forSome <#SP2_eth0> .
<#SP2_eth0> a <NetDev> .
<#SP2_eth0> <name> "eth0" .
<#SP2_eth0> <ip> "1.1.1.6" .
<#SP2_eth0> <hwAddr> "00−00−01−01−01−06" .
<#SP2_eth0> <speed> "1Gb" .
<#SP2_eth0> <type> "UTP" .
<#SP2_eth0> <connectedWith> <#sw2_p6> .

@forSome <#SPS_eth0> .
<#SPS_eth0> a <NetDev> .
<#SPS_eth0> <name> "eth0" .
<#SPS_eth0> <ip> "1.1.1.5" .
<#SPS_eth0> <hwAddr> "00−00−01−01−01−05" .
<#SPS_eth0> <speed> "1Gb" .
<#SPS_eth0> <type> "UTP" .
<#SPS_eth0> <connectedWith> <#sw2_p5> .

#models

@forSome <#simple1U> .
<#simple1U> a <Model> .
<#simple1U> <name> "AS−1042G−TF" .
<#simple1U> <size> "1U" .
<#simple1U> <power> "1400" .
<#simple1U> <cooling> "nan" .
<#simple1U> <weight> "19.5" .

@forSome <#CISCO2950> .
<#CISCO2950> a <Model> .
<#CISCO2950> <name> "Cisco Catalyst 2950−24" .
<#CISCO2950> <size> "1U" .
<#CISCO2950> <power> "30" .
<#CISCO2950> <cooling> "nan" .
<#CISCO2950> <weight> "3" .

#servers

@forSome <#SPS> .
<#SPS> a <Server> .
<#SPS> <name> "SPS" .
<#SPS> <hasDevice> <#SPS_eth0> .
<#SPS> <model> <#simple1U> .
<#SPS> <hasProgram> <#sps_mysql_3306> .
<#SPS> <hasProgram> <#sps_crypto_80> .
<#SPS> <hasProgram> <#sps_crypto_8000> .
<#SPS> <hasProgram> <#sps_514_514> .
<#SPS> <hasProgram> <#sps_199_199> .
<#SPS> <hasProgram> <#sps_sshd_22> .
<#SPS> <hasProgram> <#sps_vpn_1414> .
<#SPS> <hasProgram> <#sps_css_10060> . #client

@forSome <#SP2> .
<#SP2> a <Server> .
<#SP2> <name> "SP2" .
<#SP2> <hasDevice> <#SP2_eth0> .
<#SP2> <model> <#simple1U> .
<#SP2> <replica> <#SPS> .

```
@forSome <#CSS> .
<#CSS>  a <Server> .
<#CSS>  <name>  "CSS" .
<#CSS>  <hasDevice> <#CSS_eth0> .
<#CSS>  <model>  <#simple1U> .
<#CSS>  <hasProgram> <#css_vpn_666> .
<#CSS>  <hasProgram> <#css_srv_10060> .

@forSome <#CS2> .
<#CS2>  a <Server> .
<#CS2>  <name>  "CS2" .
<#CS2>  <hasDevice> <#CS2_eth0> .
<#CS2>  <model>  <#simple1U> .
<#CS2>  <replica> <#CSS> .

@forSome <#VPNS> .
<#VPNS>  a <Server> .
<#VPNS>  <name>  "VPNS" .
<#VPNS>  <hasDevice> <#VPNS_eth0> .
<#VPNS>  <model>  <#simple1U> .
<#VPNS>  <hasProgram> <#vpns_vpn_666> .

@forSome <#VPN2> .
<#VPN2>  a <Server> .
<#VPN2>  <name>  "VPN2" .
<#VPN2>  <hasDevice> <#VPN2_eth0> .
<#VPN2>  <model>  <#simple1U> .
<#VPN2>  <replica> <#VPNS> .

@forSome <#APMS> .
<#APMS>  a <Server> .
<#APMS>  <name>  "APMS" .
<#APMS>  <hasDevice> <#APMS_eth0> .
<#APMS>  <model>  <#simple1U> .
<#APMS>  <hasProgram> <#apms_sps_80> .
<#APMS>  <hasProgram> <#apms_sps_8000> .
<#APMS>  <hasProgram> <#apms_vpns_666> .
<#APMS>  <hasProgram> <#apms_css_666> .

@forSome <#APM2> .
<#APM2>  a <Server> .
<#APM2>  <name>  "APM2" .
<#APM2>  <hasDevice> <#APM2_eth0> .
<#APM2>  <model>  <#simple1U> .
<#APM2>  <replica> <#APMS> .

@forSome <#APM3> .
<#APM3>  a <Server> .
<#APM3>  <name>  "APM3" .
```

<#APM3> <hasDevice> <#APM3_eth0> .
<#APM3> <model> <#simple1U> .
<#APM3> <replica> <#APMS> .

@forSome <#APM4> .
<#APM4> a <Server> .
<#APM4> <name> "APM4" .
<#APM4> <replica> <#APMS> .
<#APM4> <ip> "192.168.0.0/24" .

@forSome <#X> .
<#X> a <Server> .
<#X> <name> "X" .
<#X> <hasDevice> <#X_eth0> .
<#X> <model> <#simple1U> .
<#X> <hasProgram> <#x_css_666> .
<#X> <hasProgram> <#x_sps_22> .
<#X> <hasProgram> <#x_sps_199> .
<#X> <hasProgram> <#x_sps_514> .

@forSome <#SS> .
<#SS> a <Server> .
<#SS> <name> "SS" .
<#SS> <hasDevice> <#SS_eth0> .
<#SS> <model> <#simple1U> .
<#SS> <hasProgram> <#ss_sps_1414> .

@forSome <#S2> .
<#S2> a <Server> .
<#S2> <name> "S2" .
<#S2> <hasDevice> <#S2_eth0> .
<#S2> <model> <#simple1U> .
<#S2> <replica> <#SS> .

@forSome <#S3> .
<#S3> a <Server> .
<#S3> <name> "S3" .
<#S3> <hasDevice> <#S3_eth0> .
<#S3> <model> <#simple1U> .
<#S3> <replica> <#SS> .

@forSome <#TOR> .
<#TOR> a <Server> .
<#TOR> <name> "TOR" .
<#TOR> <hasDevice> <#TOR_eth0> .
<#TOR> <model> <#simple1U> .

#

```
#nets
#

@forSome <#net1> .
<#net1>  a <Subnet> .
<#net1>  <name>  "NET1" .
<#net1>  <hasServer> <#SPS> .
<#net1>  <hasServer> <#VPNS> .
<#net1>  <hasServer> <#CSS> .
<#net1>  <hasServer> <#APMS> .

@forSome <#net2> .
<#net2>  a <Subnet> .
<#net2>  <name>  "NET2" .
<#net2>  <hasServer> <#SS> .

@forSome <#net3> .
<#net3>  a <Subnet> .
<#net3>  <name>  "NET3" .
<#net3>  <hasServer> <#X> .

#
# ports
#

@forSome <#sw1_p1> .
<#sw1_p1>  a <Port> .
<#sw1_p1>  <number>  "1" .
<#sw1_p1>  <speed>  "1Gb" .
<#sw1_p1>  <type>  "UTP" .
<#sw1_p1>  <connectedWith>  <#X_eth0> .

@forSome <#sw1_p2> .
<#sw1_p2>  a <Port> .
<#sw1_p2>  <number>  "2" .
<#sw1_p2>  <speed>  "1Gb" .
<#sw1_p2>  <type>  "UTP" .
<#sw1_p2>  <connectedWith>  <#S3_eth0> .

@forSome <#sw1_p3> .
<#sw1_p3>  a <Port> .
<#sw1_p3>  <number>  "3" .
<#sw1_p3>  <speed>  "1Gb" .
<#sw1_p3>  <type>  "UTP" .
<#sw1_p3>  <connectedWith>  <#S2_eth0> .

@forSome <#sw1_p4> .
<#sw1_p4>  a <Port> .
<#sw1_p4>  <number>  "4" .
<#sw1_p4>  <speed>  "1Gb" .
```

<#sw1_p4> <type> "UTP" .
<#sw1_p4> <connectedWith> <#SS_eth0> .

@forSome <#sw1_p5> .
<#sw1_p5> a <Port> .
<#sw1_p5> <number> "5" .
<#sw1_p5> <speed> "1Gb" .
<#sw1_p5> <type> "UTP" .
<#sw1_p5> <connectedWith> <#VPN1_eth0> .

#####

@forSome <#sw2_p1> .
<#sw2_p1> a <Port> .
<#sw2_p1> <number> "1" .
<#sw2_p1> <speed> "1Gb" .
<#sw2_p1> <type> "UTP" .
<#sw2_p1> <connectedWith> <#VPNS_eth0> .

@forSome <#sw2_p2> .
<#sw2_p2> a <Port> .
<#sw2_p2> <number> "2" .
<#sw2_p2> <speed> "1Gb" .
<#sw2_p2> <type> "UTP" .
<#sw2_p2> <connectedWith> <#VPN2_eth0> .

@forSome <#sw2_p3> .
<#sw2_p3> a <Port> .
<#sw2_p3> <number> "3" .
<#sw2_p3> <speed> "1Gb" .
<#sw2_p3> <type> "UTP" .
<#sw2_p3> <connectedWith> <#CSS_eth0> .

@forSome <#sw2_p4> .
<#sw2_p4> a <Port> .
<#sw2_p4> <number> "4" .
<#sw2_p4> <speed> "1Gb" .
<#sw2_p4> <type> "UTP" .
<#sw2_p4> <connectedWith> <#CS2_eth0> .

@forSome <#sw2_p5> .
<#sw2_p5> a <Port> .
<#sw2_p5> <number> "5" .
<#sw2_p5> <speed> "1Gb" .
<#sw2_p5> <type> "UTP" .
<#sw2_p5> <connectedWith> <#SPS_eth0> .

@forSome <#sw2_p6> .
<#sw2_p6> a <Port> .

<#sw2_p6> <number> "6" .
<#sw2_p6> <speed> "1Gb" .
<#sw2_p6> <type> "UTP" .
<#sw2_p6> <connectedWith> <#SP2_eth0> .

@forSome <#sw2_p7> .
<#sw2_p7> a <Port> .
<#sw2_p7> <number> "7" .
<#sw2_p7> <speed> "1Gb" .
<#sw2_p7> <type> "UTP" .
<#sw2_p7> <connectedWith> <#APMS_eth0> .

@forSome <#sw2_p8> .
<#sw2_p8> a <Port> .
<#sw2_p8> <number> "8" .
<#sw2_p8> <speed> "1Gb" .
<#sw2_p8> <type> "UTP" .
<#sw2_p8> <connectedWith> <#APM2_eth0> .

@forSome <#sw2_p9> .
<#sw2_p9> a <Port> .
<#sw2_p9> <number> "9" .
<#sw2_p9> <speed> "1Gb" .
<#sw2_p9> <type> "UTP" .
<#sw2_p9> <connectedWith> <#APM3_eth0> .

@forSome <#sw2_p10> .
<#sw2_p10> a <Port> .
<#sw2_p10> <number> "10" .
<#sw2_p10> <speed> "1Gb" .
<#sw2_p10> <type> "UTP" .
<#sw2_p10> <connectedWith> <#TOR_eth0> .

#
Switches
#

@forSome <#Switch2> .
<#Switch2> a <Switch> .
<#Switch2> <name> "Switch2" .
<#Switch2> <sn> "111−456" .
<#Switch2> <model> <#CISCO2950> .
<#Switch2> <mngPort> "0" .
<#Switch2> <port> <#sw2_p1> .
<#Switch2> <port> <#sw2_p2> .
<#Switch2> <port> <#sw2_p3> .
<#Switch2> <port> <#sw2_p4> .
<#Switch2> <port> <#sw2_p5> .

```
<#Switch2> <port>  <#sw2_p6> .
<#Switch2> <port>  <#sw2_p7> .
<#Switch2> <port>  <#sw2_p8> .
<#Switch2> <port>  <#sw2_p9> .
<#Switch2> <port>  <#sw2_p10> .


@forSome <#Switch1> .
<#Switch1> a <Switch> .
<#Switch1> <name>  "Switch1" .
<#Switch1> <sn>  "123-456" .
<#Switch1> <mngPort>  "0" .
<#Switch1> <model>  <#CISCO2950> .
<#Switch1> <port>  <#sw1_p1> .
<#Switch1> <port>  <#sw1_p2> .
<#Switch1> <port>  <#sw1_p3> .
<#Switch1> <port>  <#sw1_p4> .
<#Switch1> <port>  <#sw1_p5> .

#
# units
#

@forSome <#r1_u0> .
<#r1_u0> a <Unit> .
<#r1_u0> <number>  "0" .
<#r1_u0> <occupiedBy>  <#X> .

@forSome <#r1_u1> .
<#r1_u1> a <Unit> .
<#r1_u1> <number>  "1" .
<#r1_u1> <occupiedBy>  <#S3> .

@forSome <#r1_u2> .
<#r1_u2> a <Unit> .
<#r1_u2> <number>  "2" .
<#r1_u2> <occupiedBy>  <#S2> .

@forSome <#r1_u3> .
<#r1_u3> a <Unit> .
<#r1_u3> <number>  "3" .
<#r1_u3> <occupiedBy>  <#SS> .

@forSome <#r1_u4> .
<#r1_u4> a <Unit> .
<#r1_u4> <number>  "4" .
<#r1_u4> <occupiedBy>  <#Switch1> .

@forSome <#r1_u5> .
<#r1_u5> a <Unit> .
```

<#r1_u5> <number> "5" .
<#r1_u5> <occupiedBy> <#VPNS> .

@forSome <#r1_u6> .
<#r1_u6> a <Unit> .
<#r1_u6> <number> "6" .
<#r1_u6> <occupiedBy> <#VPN2> .

@forSome <#r1_u7> .
<#r1_u7> a <Unit> .
<#r1_u7> <number> "7" .
<#r1_u7> <occupiedBy> <#CSS> .

@forSome <#r1_u8> .
<#r1_u8> a <Unit> .
<#r1_u8> <number> "8" .
<#r1_u8> <occupiedBy> <#CS2> .

@forSome <#r1_u9> .
<#r1_u9> a <Unit> .
<#r1_u9> <number> "9" .
<#r1_u9> <occupiedBy> <#SPS> .

@forSome <#r1_u10> .
<#r1_u10> a <Unit> .
<#r1_u10> <number> "10" .
<#r1_u10> <occupiedBy> <#SP2> .

@forSome <#r1_u11> .
<#r1_u11> a <Unit> .
<#r1_u11> <number> "11" .
<#r1_u11> <occupiedBy> <#Switch2> .

@forSome <#r1_u12> .
<#r1_u12> a <Unit> .
<#r1_u12> <number> "12" .
<#r1_u12> <occupiedBy> <#APMS> .

@forSome <#r1_u13> .
<#r1_u13> a <Unit> .
<#r1_u13> <number> "13" .
<#r1_u13> <occupiedBy> <#APM2> .

@forSome <#r1_u14> .
<#r1_u14> a <Unit> .
<#r1_u14> <number> "14" .
<#r1_u14> <occupiedBy> <#APM3> .

@forSome <#r1_u15> .
<#r1_u15> a <Unit> .

<#r1_u15> <number> "15" .
<#r1_u15> <occupiedBy> <#TOR> .

#
Rack
#

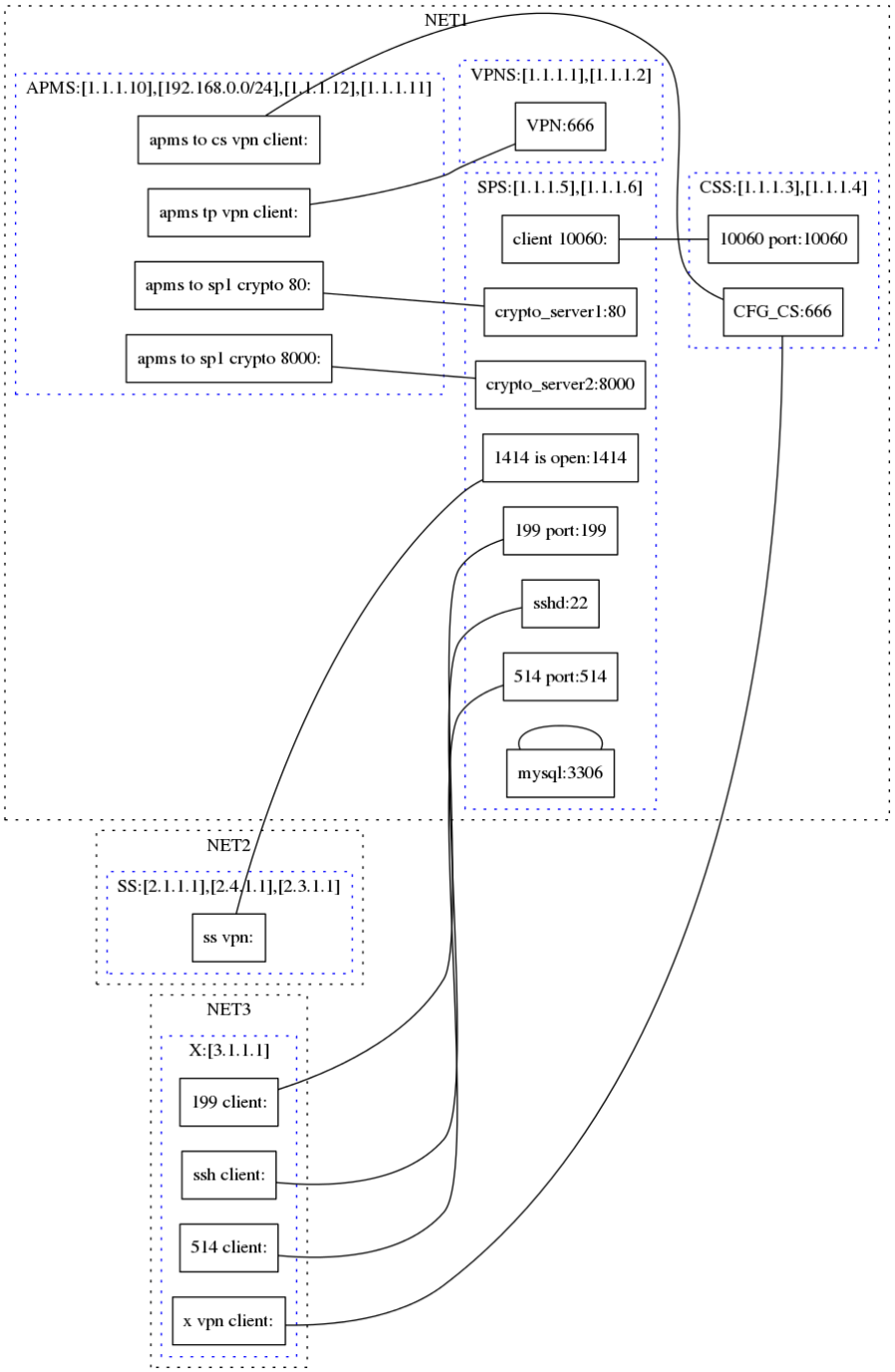
@forSome <#rack1> .
<#rack1> a <Rack> .
<#rack1> <name> "rack1" .
<#rack1> <sn> "555-55-45" .
<#rack1> <maxUnits> "25" .
<#rack1> <hasUnit> <#r1_u0> .
<#rack1> <hasUnit> <#r1_u1> .
<#rack1> <hasUnit> <#r1_u2> .
<#rack1> <hasUnit> <#r1_u3> .
<#rack1> <hasUnit> <#r1_u4> .
<#rack1> <hasUnit> <#r1_u5> .
<#rack1> <hasUnit> <#r1_u6> .
<#rack1> <hasUnit> <#r1_u7> .
<#rack1> <hasUnit> <#r1_u8> .
<#rack1> <hasUnit> <#r1_u9> .
<#rack1> <hasUnit> <#r1_u10> .
<#rack1> <hasUnit> <#r1_u11> .
<#rack1> <hasUnit> <#r1_u12> .
<#rack1> <hasUnit> <#r1_u13> .
<#rack1> <hasUnit> <#r1_u14> .
<#rack1> <hasUnit> <#r1_u15> .

Listing 2: sid-msg.map

```
6000000|| Wrong port connection
6000001|| Wrong port connection
6000002|| Wrong port connection
6000003|| Wrong port connection
6000004|| Wrong port connection
6000005|| Wrong port connection
6000006|| Wrong port connection
6000007|| Wrong port connection
6000008|| Outgoing connection to illegal IP
6000009|| Incomming connection from illegal IPs
6000010|| Outgoing connection to illegal IP
6000011|| Incomming connection from illegal IPs
6000012|| Outgoing connection to illegal IP
6000013|| Incomming connection from illegal IPs
6000014|| Outgoing connection to illegal IP
6000015|| Incomming connection from illegal IPs
6000016|| Wrong hw addr
6000017|| Wrong hw addr
6000018|| Wrong hw addr
6000019|| Wrong hw addr
6000020|| Wrong hw addr
6000021|| Wrong hw addr
6000022|| Wrong hw addr
6000023|| Wrong hw addr
6000024|| Wrong hw addr
6000025|| Wrong hw addr
6000026|| Wrong hw addr
6000027|| Wrong hw addr
6000028|| Wrong hw addr
6000029|| Wrong hw addr
```

Listing 3: Rules

```
#−−−output−−−
alert tcp [[2.1.1.1],[2.4.1.1],[2.3.1.1]] any −> [[1.1.1.5],[1.1.1.6]] ![1414] (msg:" Wrong port connection"; rev:1;
alert tcp [[1.1.1.5],[1.1.1.6]] any −> [[1.1.1.3],[1.1.1.4]] ![10060] (msg:" Wrong port connection"; rev:1; classty
alert tcp [[1.1.1.5],[1.1.1.6]] any −> [[1.1.1.5],[1.1.1.6]] ![3306] (msg:" Wrong port connection"; rev:1; classtyp
alert tcp [[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]] any −> [[1.1.1.5],[1.1.1.6]] ![80, 8000] (msg:" Wrong
alert tcp [[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]] any −> [[1.1.1.1],[1.1.1.2]] ![666] (msg:" Wrong port
alert tcp [[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]] any −> [[1.1.1.3],[1.1.1.4]] ![666] (msg:" Wrong port
alert tcp [[3.1.1.1]] any −> [[1.1.1.5],[1.1.1.6]] ![22, 514, 199] (msg:" Wrong port connection"; rev:1; classtype
alert tcp [[3.1.1.1]] any −> [[1.1.1.3],[1.1.1.4]] ![666] (msg:" Wrong port connection"; rev:1; classtype:tcp−co
#−−−overall−−−
alert tcp [[2.1.1.1],[2.4.1.1],[2.3.1.1]] any −> ![[1.1.1.5],[1.1.1.6]] any (msg:" Outgoing connections to illegal I
alert tcp ![[1.1.1.5],[1.1.1.6]] any −> [[2.1.1.1],[2.4.1.1],[2.3.1.1]] any (msg:" Incomming connections from illeg
alert tcp [[1.1.1.5],[1.1.1.6]] any −> ![[1.1.1.3],[1.1.1.4], [1.1.1.5],[1.1.1.6]] any (msg:" Outgoing connections to
alert tcp ![[1.1.1.3],[1.1.1.4], [1.1.1.5],[1.1.1.6]] any −> [[1.1.1.5],[1.1.1.6]] any (msg:" Incomming connections
alert tcp [[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]] any −> ![[1.1.1.5],[1.1.1.6], [1.1.1.1],[1.1.1.2], [1.1.1.3]
alert tcp ![[1.1.1.5],[1.1.1.6], [1.1.1.1],[1.1.1.2], [1.1.1.3],[1.1.1.4]] any −> [[1.1.1.10],[192.168.0.0/24],[1.1.1.12],
alert tcp [[3.1.1.1]] any −> ![[1.1.1.5],[1.1.1.6], [1.1.1.3],[1.1.1.4]] any (msg:" Outgoing connections to illegal I
alert tcp ![[1.1.1.5],[1.1.1.6], [1.1.1.3],[1.1.1.4]] any −> [[3.1.1.1]] any (msg:" Incomming connections from ille
#−−−hw_addr−−−
alert ip [1.1.1.12] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−12;rev:1; sid:60000
alert ip [3.1.1.1] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−03−01−01−01;rev:1; sid:6000017
alert ip [2.3.1.1] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−02−03−01−01;rev:1; sid:6000018
alert ip [2.4.1.1] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−02−04−01−01;rev:1; sid:6000019
alert ip [1.1.1.2] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−02;rev:1; sid:6000020
alert ip [1.1.1.254] any −> any any (msg:" Wrong hw addr"; eth_src:01−01−01−02−05−04;rev:1; sid:60000
alert ip [1.1.1.4] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−04;rev:1; sid:6000022
alert ip [1.1.1.5] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−05;rev:1; sid:6000023
alert ip [1.1.1.1] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−01;rev:1; sid:6000024
alert ip [1.1.1.10] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−10;rev:1; sid:600002
alert ip [1.1.1.11] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−11;rev:1; sid:600002
alert ip [1.1.1.3] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−03;rev:1; sid:6000027
alert ip [2.1.1.1] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−02−01−01−01;rev:1; sid:6000028
alert ip [1.1.1.6] any −> any any (msg:" Wrong hw addr"; eth_src:00−00−01−01−01−06;rev:1; sid:6000029
```


NET1
APMS:[1.1.1.10],[192.168.0.0/24],[1.1.1.12],[1.1.1.11]
apms to cs vpn client:
apms tp vpn client:
apms to sp1 crypto 80:
apms to sp1 crypto 8000:
VPNS:[1.1.1.1],[1.1.1.2]
VPN:666
SPS:[1.1.1.5],[1.1.1.6]
client 10060:
crypto_server1:80
crypto_server2:8000
1414 is open:1414
199 port:199
sshd:22
514 port:514
mysql:3306
CSS:[1.1.1.3],[1.1.1.4]
10060 port:10060
CFG_CS:666
NET2
SS:[2.1.1.1],[2.4.1.1],[2.3.1.1]
ss vpn:
NET3
X:[3.1.1.1]
199 client:
ssh client:
514 client:
x vpn client: