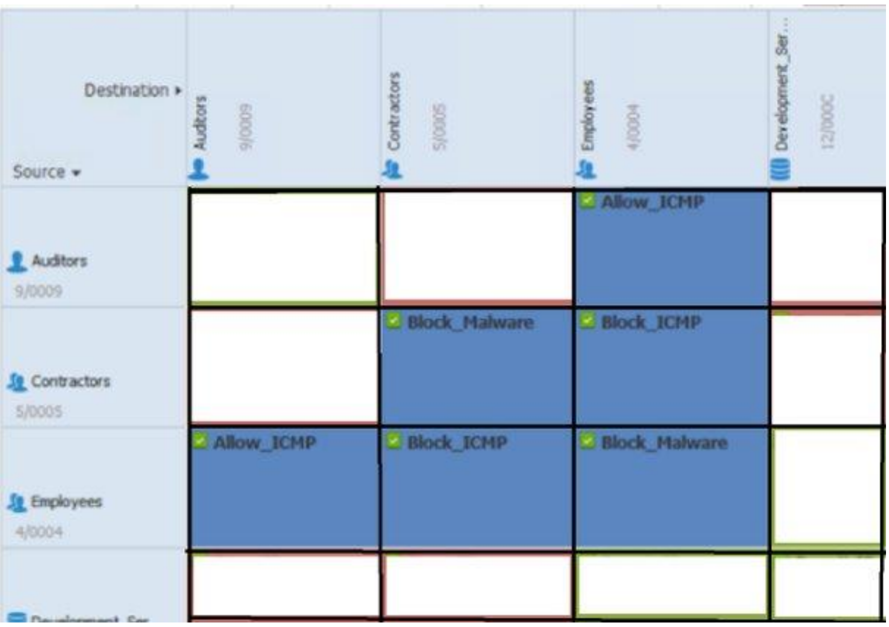
Problem statement

Security is a very important aspect of our networks today. Ensuring that the network doesn't get subjected to cyber-attacks from inside or outside is a key responsibility of the security features. One such feature is Cisco Trust Sec where each endpoint in the network is identified as belonging to a group and strict rules are written to define which group can talk to which other. This will enable us to track conversations between all endpoints. Today we represent these rules in a matrix with the columns representing destination groups and rows representing source groups and the intersecting cells holding the rule of engagement between the two. You can assume that a group is represented by a number (range 0 to 65536) As an example, the representation could be in the form of a matrix where the rows and columns represent source and destination groups and the intersecting cells defined the rules. This representation can get very cumbersome and huge and unmanageable when the rules run into 1000s.



Destination ▸ Source ▾	Auditors 9/0009	Contractors 5/0005	Employees 4/0004	Development_Ser... 12/000C
Auditors 9/0009			Allow_ICMP	
Contractors 5/0005		Block_Malware	Block_ICMP	
Employees 4/0004	Allow_ICMP	Block_ICMP	Block_Malware	
Development_Ser				

Requirements

The ask of this problem is to come up with unique, innovative visualization of these rules of engagement which is easy to understand and most importantly efficient in terms of loading on the screen. We invite you to use your imagination and coding skills to come up with a creative and effective solution.

Input

The team will be required to generate the input for the problem.

The format is defined as follows:

ACL definition

```
ip access-list role-based {name of access-list}    <<< access-list

   permit/deny {   <0-255>  An IP protocol number    <<< rule

  ahp      Authentication Header Protocol

  eigrp    Cisco's EIGRP routing protocol

  esp      Encapsulation Security Payload

  gre      Cisco's GRE tunneling

  icmp     Internet Control Message Protocol

  igmp     Internet Gateway Message Protocol

  ip       Any Internet Protocol

  ipinip   IP in IP tunneling

  nos      KA9Q NOS compatible IP over IP tunneling

  ospf     OSPF routing protocol

  pcp      Payload Compression Protocol

  pim      Protocol Independent Multicast

  tcp      Transmission Control Protocol

  udp      User Datagram Protocol }
```

CTS role based permission definition

```
cts role-based permissions from {sgt_num | unknown} to {dgt_num | unknown} {permit | deny}
```

Example file input:

```
Ip access-list role-based Allow_ICMP
   10 permit icmp
Ip access-list role-based Block_ICMP
    10 deny icmp
Ip access-list role-based Block_Malware
    10 deny 45
    20 deny 93


Cts role-based permissions from 9 to 4 Allow_ICMP
Cts role-based permissions from 5 to 5 Block_Malware
Cts role-based permissions from 5 to 4 Block_ICMP
Cts role-based permissions from 4 to 9 Allow_ICMP
```

Cts role-based permissions from 4 to 5 Block_ICMP
Cts role-based permissions from 4 to 4 Allow_Malware

The team should also generate various combinations to test different aspects of visualization.

Size of Input

- 500 access-lists
- With a min of 1 and max of 20 rules in each
- Combination of port numbers and use every protocol at least 10 times
- 10,000 cts role based permissions

Output

The ask is to come up with a visualization in any format that the team sees fit and it will be evaluated on the criteria below.

Evaluation criteria

- Visualization load time
- Intuitiveness of the rendering
- Ease of search and browsing. Search based on group numbers, applications denied and permitted etc.
- Smooth transition to and from summary and detailed views
- Creative and out of the box thinking