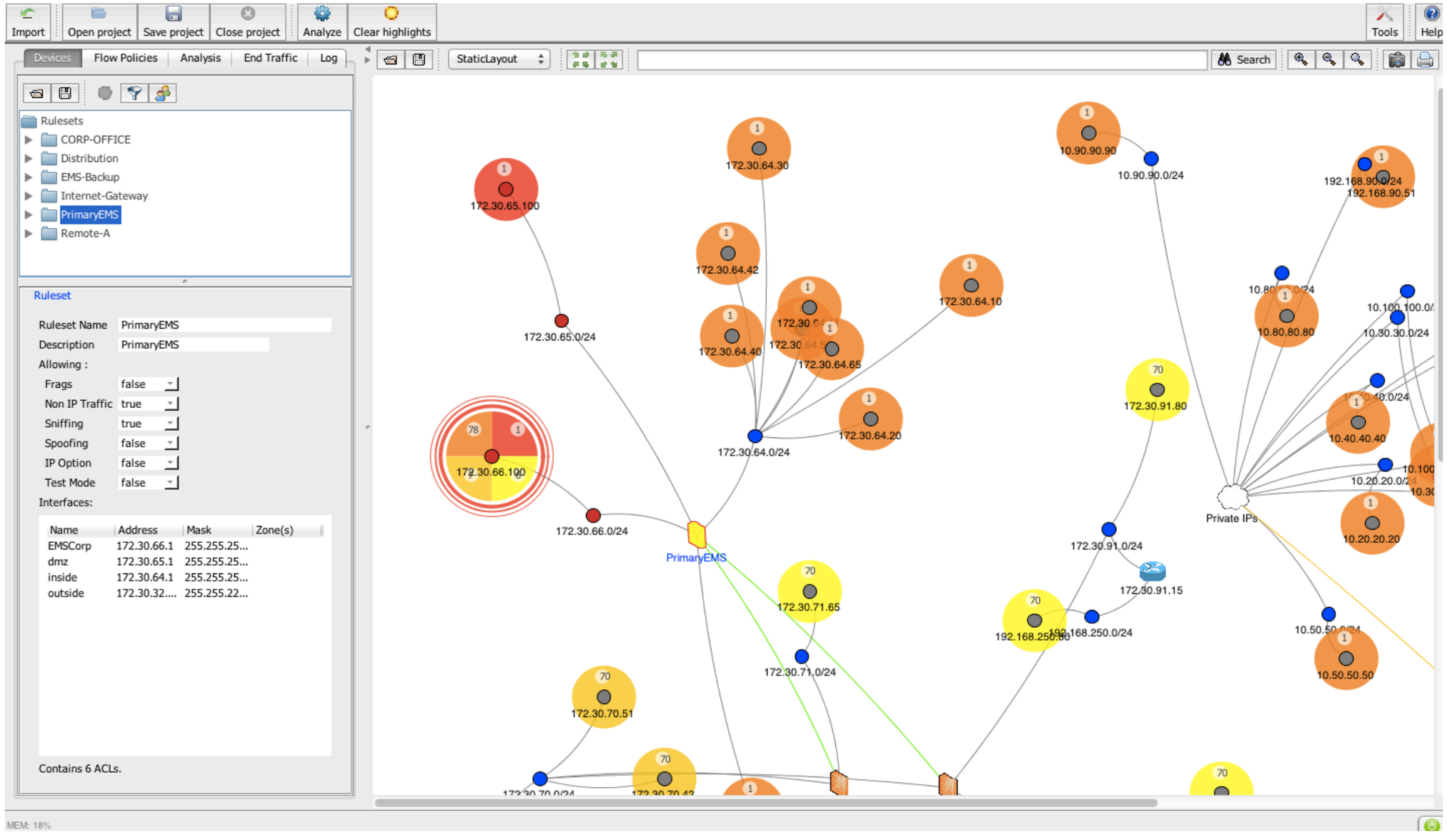
# Visualizing Network Security Policy with NP-View



# History

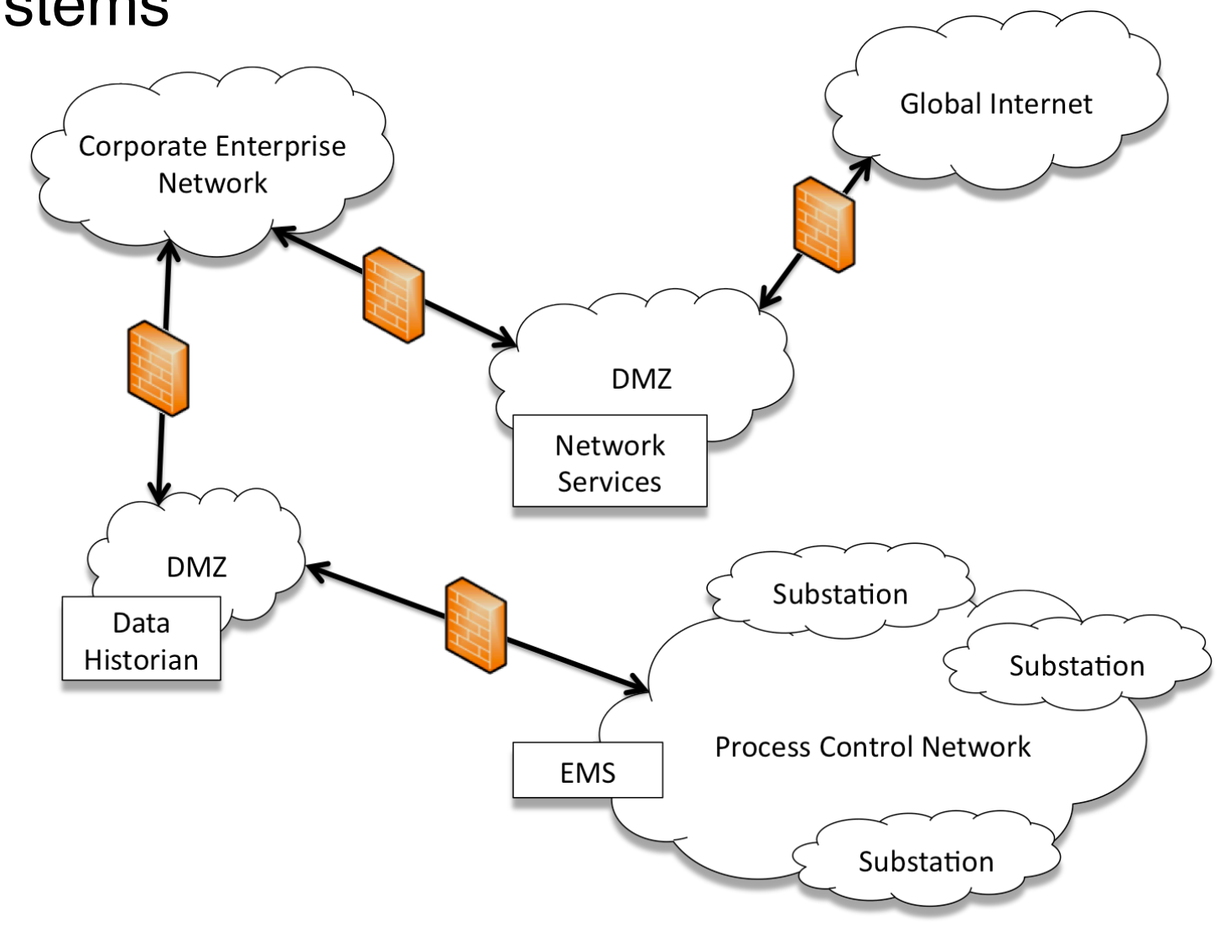

- PhD thesis project by Sankalp Singh, started in 2006
  - *Automatic Verification of Security Policy Implementations*, 2012

- Graduated TCIPG project, tech transfer grant from DHS in 2012

- Network Perception startup launched in 2014 at UIUC incubator
  - Co-founded by Mouna Bamba, Robin Berthier, David Nicol, Edmond Rogers, Bill Sanders

# Motivation: Critical Infrastructure Protection

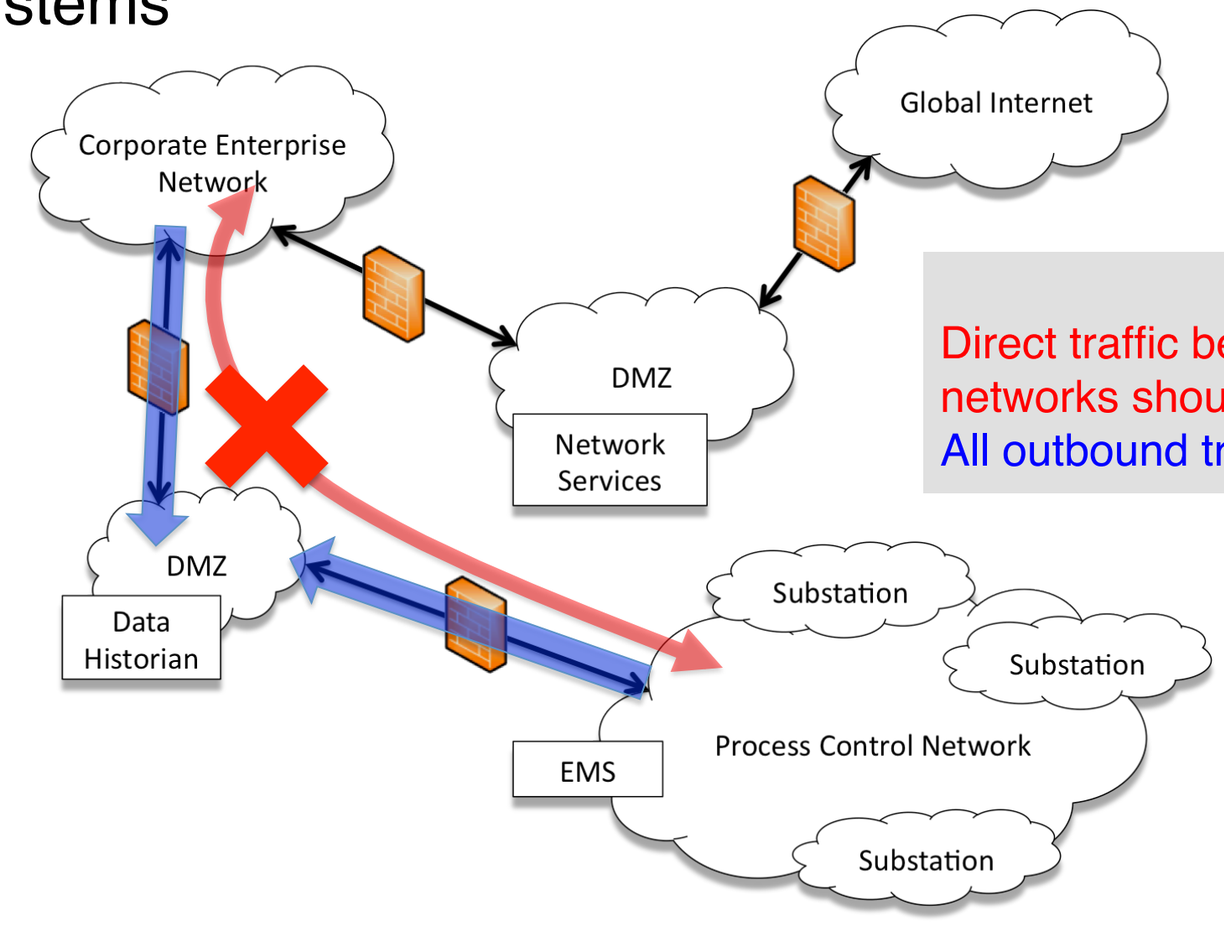
- Process control networks are increasingly connected to other networks in enterprise systems




- Accesses controlled by configuring potentially many firewalls

# Motivation: Critical Infrastructure Protection

- Process control networks are increasingly connected to other networks in enterprise systems




Policy rules:

Direct traffic between Corporate and Control networks should be prevented

All outbound traffic should end in DMZ

- Accesses controlled by configuring potentially many firewalls

# Motivation: Critical Infrastructure Protection

- NERC CIP standards regulations introduced to reduce risks of cyber attacks

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION**

October 31, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

| Region | Registered Entity | NOC ID | NERC Violation ID | Reliability Std. | Req. | VRF | Total Penalty |
|---|---|---|---|---|---|---|---|
| Reliability*First* Corporation | URE1 | 1448 | RFC201100957 | CIP-002-1 | R1 | Medium[5] | $725,000 |
| Reliability*First* Corporation | URE1 | 1448 | RFC201100958 | CIP-002-1 | R2 | High[6] | |

*http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-1448.pdf*

# Firewall Audit Process

- Complex set of rules and parameters stored in configuration files

```
ASA Version 9.0
hostname TEST_FIREWALL

!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! DEFINITION OF INTERFACES !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!

interface Ethernet0/1
 speed 100
 duplex full
 nameif corporate
 security-level 100
 ip address 172.30.0.1
255.255.255.0
!
interface Ethernet0/2
 speed 100
 duplex full
 nameif scada
 security-level 15
 ip address 10.0.0.1
255.255.255.0
!
interface Ethernet0/3
 speed 100
 duplex full
 nameif remote
 security-level 15
 ip address 192.168.0.1
255.255.255.0
!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! DEFINITION OF OBJECT GROUP !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

object-group network GROUP1
 network-object host 172.30.0.2
!
object-group network GROUP2
 network-object host 10.0.0.2
 network-object host 10.0.0.3
 network-object host 10.0.0.4
 network-object host 10.0.0.5
 network-object host 10.0.0.6
!
object-group network GROUP3
 network-object host
192.168.0.2
 network-object host
192.168.0.3
 network-object host
192.168.0.4
!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! DEFINITION OF ACCESS RULES !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

access-list FromCorporate
extended deny tcp object-group
GROUP1 10.0.0.0 255.0.0.0 eq
www
access-list FromCorporate
extended permit tcp object-
group GROUP1 any eq www
inactive
access-list FromCorporate
extended permit tcp object-
group GROUP1 any eq ftp
access-list 124 permit udp
10.0.0.1 255.255.255.255
10.0.1.1 255.255.255.255 range
135 netbios-ss

!!!!!!!!!!!!!!!!!!!!
! BINDING OF RULES !
!!!!!!!!!!!!!!!!!!!!

access-group FromCorporate in
interface corporate
```

# Firewall Audit Process (cont.)

- Each firewall has a collection of Object *Group* definitions and *Access Control Lists (ACLs)*
- Each ACL bound to a particular interface
- ACLs are comprised of list of *rules*, processed sequentially
- Each rule is of the form <*P*, *action*>
  - *P*: predicate characterizing the attributes of the traffic (protocol, source, destination)
  - *action*: {*accept*, *deny*, *drop*}

| Rule Id. | Protocol | Source | Destination | Action |
|---|---|---|---|---|
| 1. | tcp | 10.1.1.0/25 | Any | Deny |
| 2. | udp | Any | 192.168.1.0/24 | Accept |
| 3. | tcp | 10.1.1.128/25 | Any | Deny |
| 4. | udp | 172.16.1.0/24 | 192.168.1.0/24 | Deny |
| 5. | tcp | 10.1.1.0/24 | Any | Accept |
| 6. | udp | 10.1.1.0/24 | 192.168.0.0/16 | Deny |
| 7. | udp | 172.16.1.0/24 | Any | Accept |

# NP-View: lightweight offline network audit tool

Input → Review Process → Output

Backup-EMS Firewall

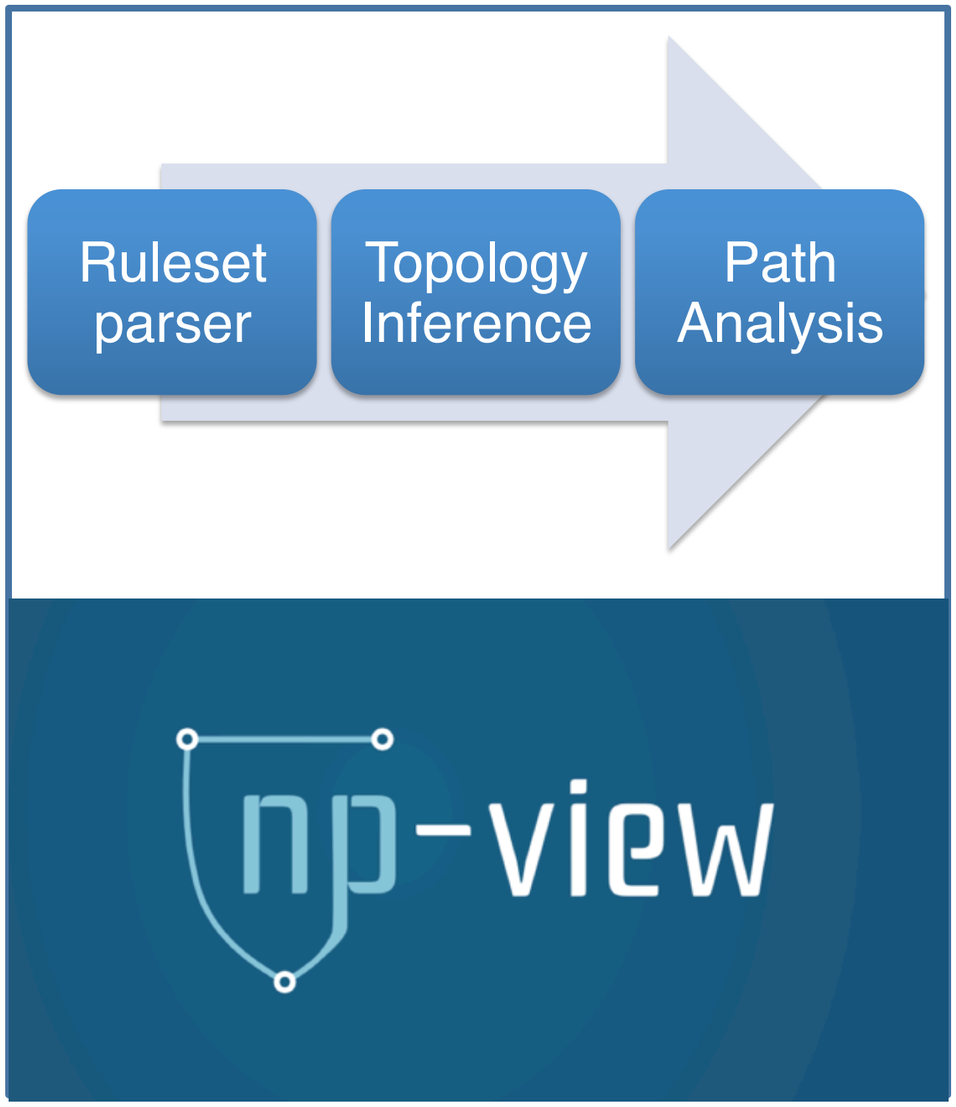
Main Corp. Firewall

Distributi on Firewall

Primary EMS Firewall

Internet Firewall

Remote Access Firewall



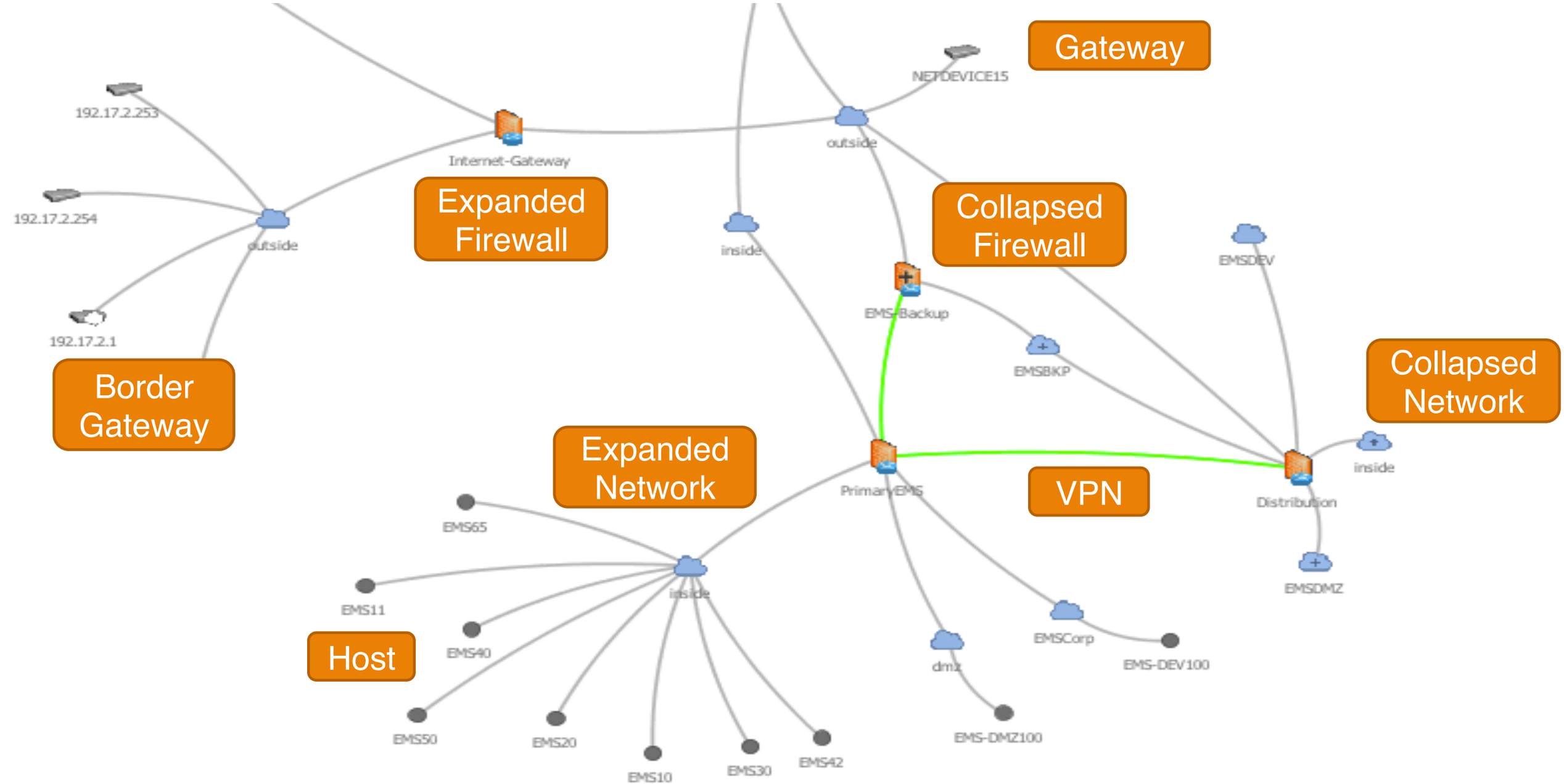

Project Report

Rule table

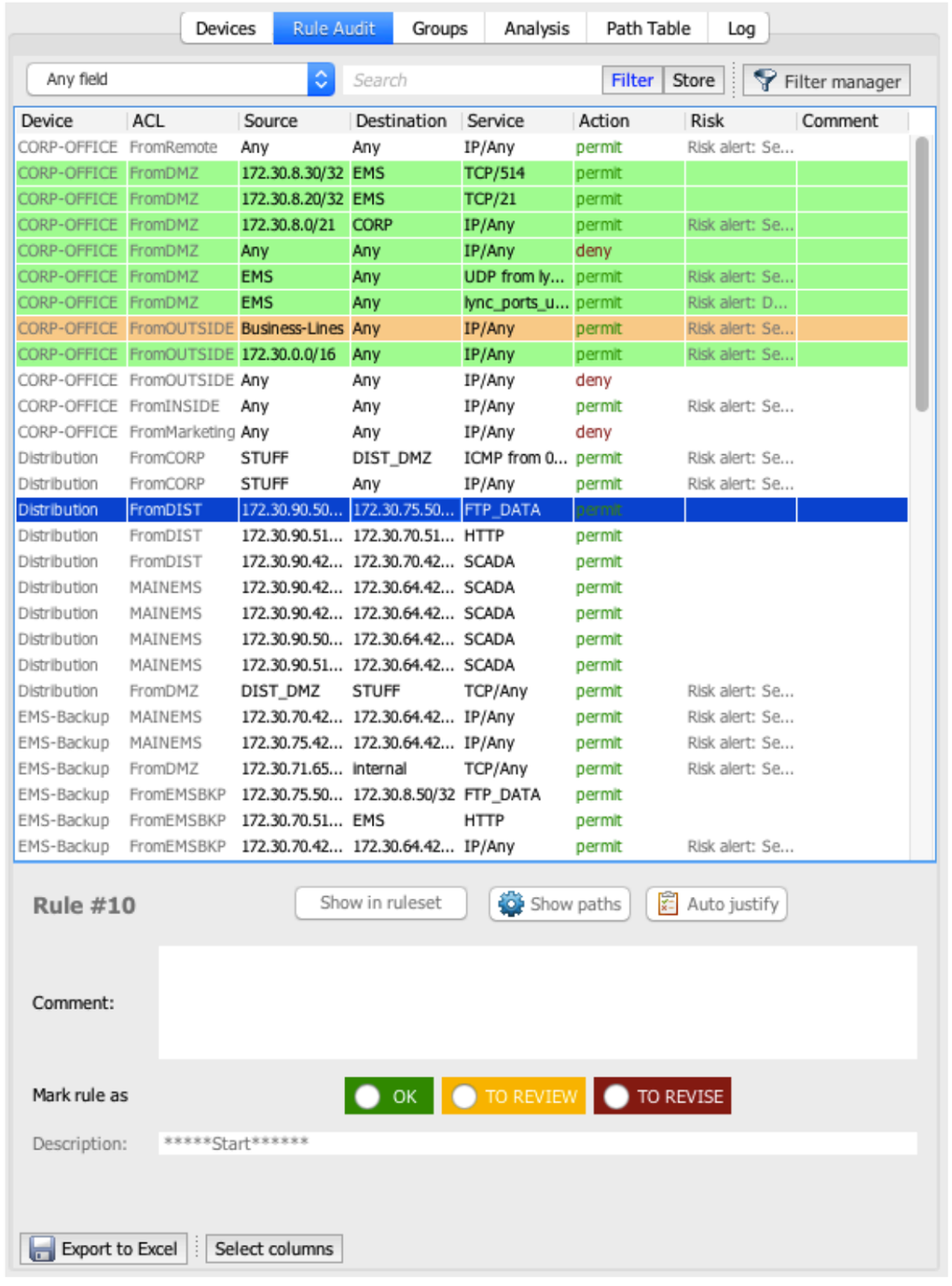
Path tables

Network Maps

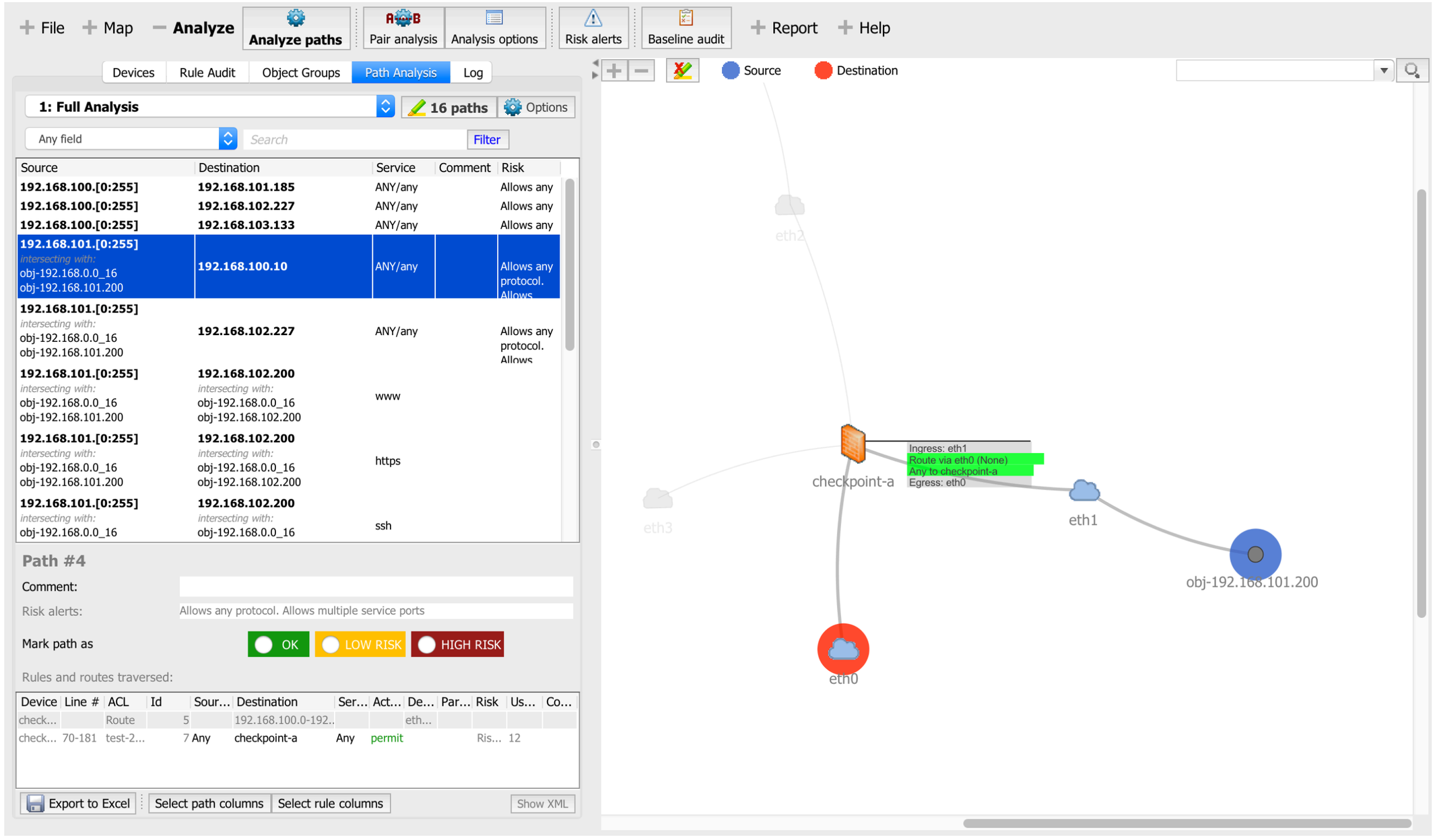
# Topology Map



# Rule Audit


Devices
Rule Audit
Groups
Analysis
Path Table
Log
Any field
Search
Filter
Store
Filter manager
Device ACL Source Destination Service Action Risk Comment
CORP-OFFICE FromRemote Any Any IP/Any permit Risk alert: Se...
CORP-OFFICE FromDMZ 172.30.8.30/32 EMS TCP/514 permit
CORP-OFFICE FromDMZ 172.30.8.20/32 EMS TCP/21 permit
CORP-OFFICE FromDMZ 172.30.8.0/21 CORP IP/Any permit Risk alert: Se...
CORP-OFFICE FromDMZ Any Any IP/Any deny
CORP-OFFICE FromDMZ EMS Any UDP from ly... permit Risk alert: Se...
CORP-OFFICE FromDMZ EMS Any lync_ports_u... permit Risk alert: D...
CORP-OFFICE FromOUTSIDE Business-Lines Any IP/Any permit Risk alert: Se...
CORP-OFFICE FromOUTSIDE 172.30.0.0/16 Any IP/Any permit Risk alert: Se...
CORP-OFFICE FromOUTSIDE Any Any IP/Any deny
CORP-OFFICE FromINSIDE Any Any IP/Any permit Risk alert: Se...
CORP-OFFICE FromMarketing Any Any IP/Any deny
Distribution FromCORP STUFF DIST_DMZ ICMP from 0... permit Risk alert: Se...
Distribution FromCORP STUFF Any IP/Any permit Risk alert: Se...
Distribution FromDIST 172.30.90.50... 172.30.75.50... FTP_DATA permit
Distribution FromDIST 172.30.90.51... 172.30.70.51... HTTP permit
Distribution FromDIST 172.30.90.42... 172.30.70.42... SCADA permit
Distribution MAINEMS 172.30.90.42... 172.30.64.42... SCADA permit
Distribution FromDIST 172.30.90.42... 172.30.70.42... SCADA permit
Distribution MAINEMS 172.30.90.42... 172.30.64.42... SCADA permit
Distribution MAINEMS 172.30.90.42... 172.30.64.42... SCADA permit
Distribution MAINEMS 172.30.90.50... 172.30.64.42... SCADA permit
Distribution MAINEMS 172.30.90.51... 172.30.64.42... SCADA permit
Distribution FromDMZ DIST_DMZ STUFF TCP/Any permit Risk alert: Se...
EMS-Backup MAINEMS 172.30.70.42... 172.30.64.42... IP/Any permit Risk alert: Se...
EMS-Backup MAINEMS 172.30.75.42... 172.30.64.42... IP/Any permit Risk alert: Se...
EMS-Backup FromDMZ 172.30.71.65... Internal TCP/Any permit Risk alert: Se...
EMS-Backup FromEMSBKP 172.30.75.50... 172.30.8.50/32 FTP_DATA permit
EMS-Backup FromEMSBKP 172.30.70.51... EMS HTTP permit
EMS-Backup FromEMSBKP 172.30.70.42... 172.30.64.42... IP/Any permit Risk alert: Se...
Rule #10
Show in ruleset
Show paths
Auto justify
Comment:
Mark rule as
OK
TO REVIEW
TO REVISE
Description:
*****Start******
Export to Excel
Select columns

# Path Analysis



# Path Data Structure

- Path #
- Protocol
- **Source information:**
  - Source Range
  - Source Hosts
  - Source Network
  - Source Firewall
  - Source Port
- **Destination information:**
  - Destination Range
  - Destination Hosts
  - Destination Network
  - Destination Firewall
  - Destination Port
- Service
- Comment
- Risk
- Marker
- Rules

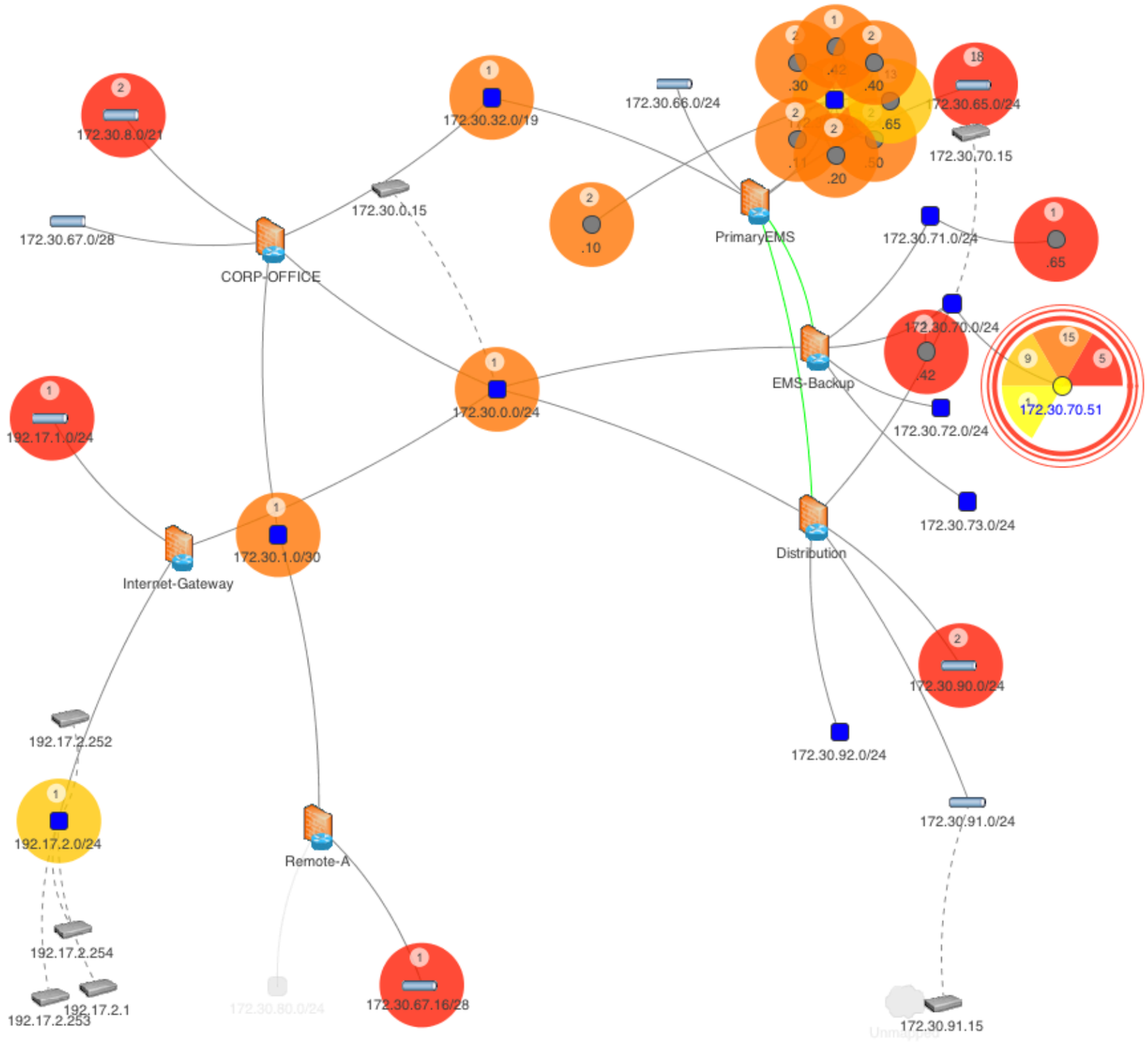
**Ranges** are mathematically computed by the engine

**Hosts** are IP found in the map from the range

**Networks** are the parent subnet containing the range

**Firewalls** are the first or last device crossed

# Stepping-stone Attack Map



# Roadmap

- Support for additional network layers
  - Layer 2 (switches, VLANs)
  - Layer 7 (application-layer firewalls)

- Change tracking of rulesets over time
  - Topology diff viewer
  - Path analysis impact

- Importing additional network data
  - Nmap scan
  - Wireshark traces

# Publications

## Patent

- S. Singh, D. M. Nicol, W. H. Sanders, and M. Seri. Analysis of Distributed Policy Rule-Sets for Compliance with Global Policy. *Provisional Patent Application* in TF070703, BHGL 10322-99, Serial Number 60/941, 132, June 2007.

## Papers

- D. M. Nicol, W. H. Sanders, S. Singh, and M. Seri. Usable Global Network Access Policy for PCS. *IEEE Security and Privacy*, 6(6), November-December, 2008, pp. 30-36.
- D. M. Nicol, W. H. Sanders, S. Singh, and M. Seri. Experiences Validating the Access Policy Tool in Industrial Settings. In *Proceedings of the 43rd Annual Hawai'i International Conference on System Sciences (HICSS)*, Koloa, Kauai, Hawaii, January 5-8, 2010, pp. 1-8.
- R. K. Cunningham, S. Cheung, M. Fong, U. Lindqvist, D. M. Nicol, R. Pawlowski, E. Robinson, W. H. Sanders, S. Singh, A. Valdes, B. Woodworth, and M. Zhivich. Securing Process Control Systems of Today and Tomorrow. In *Proceedings of the IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Hanover, NH, March 2007.
- S. Singh, D. M. Nicol, W. H. Sanders, and M. Seri. Verifying SCADA Network Access Control Policy Implementations Using the Access Policy Tool. In *Proceedings of the IFIP WG 11.10 International Conference on Critical Infrastructure Protection,* Hanover, NH, March 2007.

# Questions?


Robin Berthier

rgb@illinois.edu

rgb@network-perception.com