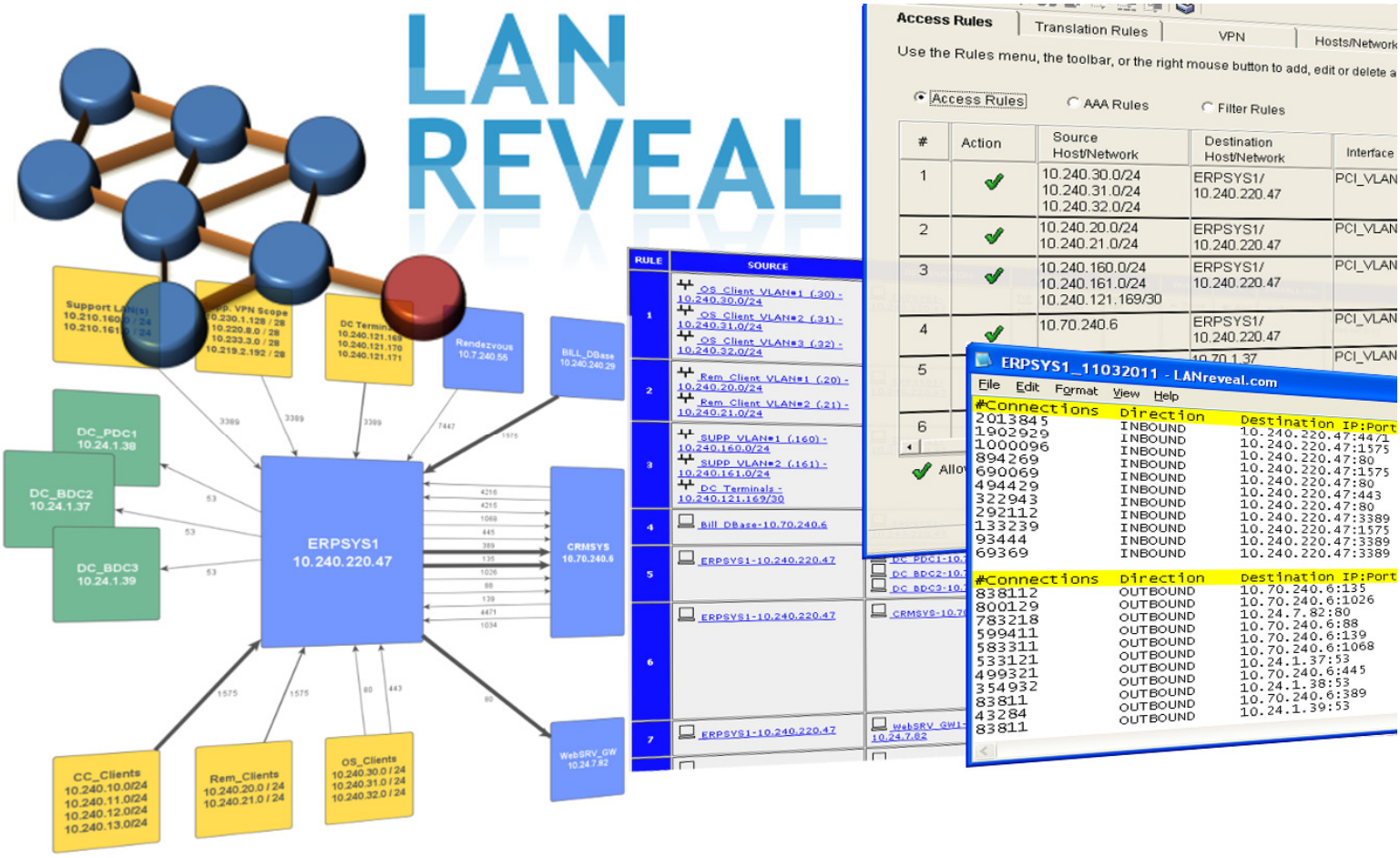



**LANreveal offers a simple and convenient way to understand and map your network. Using our revolutionary technology, LANreveal can help you to regain control of your network, allowing you to protect your enterprise accordingly.**

**You can rely on LANreveal to prevent cyber threats, reduce risk exposure and demonstrate compliance with regulations such as PCI:DSS, ISO27001 and Sarbanes Oxley (SOX).**

## LANreveal - Where to start?

Every year, companies spend millions of pounds on security devices and services to prevent unauthorised access to their network.
Despite this security breaches occur with alarming frequency, often leaving security managers wondering exactly what is going on with their network.
This can make firewall configuration extremely tricky and may cause issues at audit time.

To have confidence in your network security, you need to know ***exactly*** what access is, *and is not* allowed to pass through your infrastructure. With LANreveal you will know precisely what access is allowed between different security zones, and to all of your critical systems.

LANreveal collects information across your networks, normalizes the data, and produces detailed visual maps of the network topology. LANreveal is designed to support PCI DSS v2.0 (specifically Sections 1.1, 1.2, 1.3, 2.2 & 2.3)

Using LANreveal is a simple way to regain control of your firewalls, and accurately understand exactly what is happening on your network **today.**

"Without a doubt, the deployment of LANreveal has been of significant benefit to Virgin Mobile.

As a direct result of using LANreveal we were easily able to understand the traffic interconnection profile of our enterprise.

Having this knowledge allowed us to build a PCI compliant firewall configuration."

**Mr. Simon Hoscik**
**Information Security,**
**Virgin Mobile**

## What we do.

Using our revolutionary technology, LANreveal can help you to better understand your network. Our software will help you to visualize your network traffic, and identify areas of concern.
LANreveal's unique combination of intelligent automation and complete network visibility offers an alternative to error prone manual processes traditionally used to perform auditing for compliance.
Our security solutions are used in the most demanding network environments, and are built to the very highest standards. We can help you to understand your network, help you understand how business processes map to network traffic and ultimately help you to protect your enterprise accordingly.

## Features

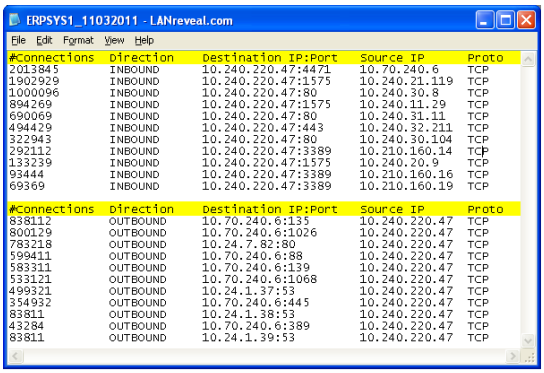
+ **Agents for all common platforms**
+ **Real-time data collection**
+ **Simple to deploy**
+ **Very low resource overhead**
+ **Rules can be imported directly into Checkpoint® or Cisco® firewalls**

## How does it work?

LANreveal is an agent based network discovery application.
We have agents available for almost all operating systems (including MS Windows, Solaris, HPUX, AIX and Linux)
These agents are written in a number of different languages depending on the host operating system, but in all cases are humanly readable script - *not invisible compiled code*, meaning that you are able to see clearly what the agent is doing.
The agents are left to collect data for a period of time *(normally around a month)* after which time the resulting data is collected and processed off-site using our bespoke engine software.
Off-site processing is used for a number of reasons, the main being that the agents (by design) have *very-very* low CPU and resource requirements, which ensures that using LANreveal won't interfere with your day-to-day business operations.
Processing the resulting data, however is exceptionally processor intensive and so we conduct this off-site using our secure bespoke and purpose built processing facility.
Once the data has been collected and processed, it can be represented in many different ways - some examples of which are given below.

## Network Documentation

The simplest form being simply a text file containing information on the observed connections, along with their relative frequency.
LANreveal can output information as a simple text file containing a list of **Inbound** and **Outbound** connections ordered by relative frequency and presented in an easy to read format, including source and destination IP/Hostname, port number, protocol and frequency.
Although simple, this report gives valuable insight into a server (or servers) interconnections.

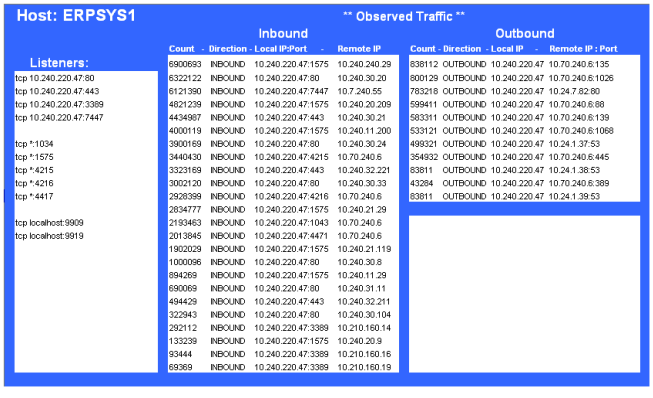


ERPSYS1_11032011 - LANreveal.com

File Edit Format View Help

| #Connections | Direction | Destination IP:Port | Source IP | Proto |
|---|---|---|---|---|
| 2013845 | INBOUND | 10.240.220.47:4471 | 10.70.240.6 | TCP |
| 1902929 | INBOUND | 10.240.220.47:1575 | 10.240.21.119 | TCP |
| 1000096 | INBOUND | 10.240.220.47:80 | 10.240.30.8 | TCP |
| 894269 | INBOUND | 10.240.220.47:1575 | 10.240.11.29 | TCP |
| 690069 | INBOUND | 10.240.220.47:80 | 10.240.31.11 | TCP |
| 494429 | INBOUND | 10.240.220.47:443 | 10.240.32.211 | TCP |
| 322943 | INBOUND | 10.240.220.47:80 | 10.240.30.104 | TCP |
| 292112 | INBOUND | 10.240.220.47:3389 | 10.210.160.14 | TCP |
| 133239 | INBOUND | 10.240.220.47:1575 | 10.240.20.9 | TCP |
| 93444 | INBOUND | 10.240.220.47:3389 | 10.210.160.16 | TCP |
| 69369 | INBOUND | 10.240.220.47:3389 | 10.210.160.19 | TCP |

| #Connections | Direction | Destination IP:Port | Source IP | Proto |
|---|---|---|---|---|
| 838112 | OUTBOUND | 10.70.240.6:135 | 10.240.220.47 | TCP |
| 800129 | OUTBOUND | 10.70.240.6:1026 | 10.240.220.47 | TCP |
| 783218 | OUTBOUND | 10.24.7.82:80 | 10.240.220.47 | TCP |
| 599411 | OUTBOUND | 10.70.240.6:88 | 10.240.220.47 | TCP |
| 583311 | OUTBOUND | 10.70.240.6:139 | 10.240.220.47 | TCP |
| 533121 | OUTBOUND | 10.70.240.6:1068 | 10.240.220.47 | TCP |
| 499321 | OUTBOUND | 10.24.1.37:53 | 10.240.220.47 | TCP |
| 354932 | OUTBOUND | 10.70.240.6:445 | 10.240.220.47 | TCP |
| 83811 | OUTBOUND | 10.24.1.38:53 | 10.240.220.47 | TCP |
| 43284 | OUTBOUND | 10.70.240.6:389 | 10.240.220.47 | TCP |
| 83811 | OUTBOUND | 10.24.1.39:53 | 10.240.220.47 | TCP |



Host: ERPSYS1 — ** Observed Traffic **

Listeners:

tcp 10.240.220.47:80
tcp 10.240.220.47:443
tcp 10.240.220.47:3389
tcp 10.240.220.47:7447
tcp *:1034
tcp *:1575
tcp *:4215
tcp *:4216
tcp *:4417
tcp localhost:9909
tcp localhost:9919

Inbound

| Count | Direction | Local IP:Port | Remote IP |
|---|---|---|---|
| 6900693 | INBOUND | 10.240.220.47:1575 | 10.240.240.29 |
| 6322122 | INBOUND | 10.240.220.47:80 | 10.240.30.20 |
| 6121380 | INBOUND | 10.240.220.47:7447 | 10.7.240.55 |
| 4821239 | INBOUND | 10.240.220.47:1575 | 10.240.20.209 |
| 4434987 | INBOUND | 10.240.220.47:443 | 10.240.30.21 |
| 4000119 | INBOUND | 10.240.220.47:1575 | 10.240.11.200 |
| 3900169 | INBOUND | 10.240.220.47:80 | 10.240.30.24 |
| 3440430 | INBOUND | 10.240.220.47:4215 | 10.70.240.6 |
| 3323169 | INBOUND | 10.240.220.47:443 | 10.240.32.221 |
| 3002120 | INBOUND | 10.240.220.47:80 | 10.240.30.33 |
| 2928399 | INBOUND | 10.240.220.47:4216 | 10.70.240.6 |
| 2834777 | INBOUND | 10.240.220.47:1575 | 10.240.21.29 |
| 2193463 | INBOUND | 10.240.220.47:1043 | 10.70.240.6 |
| 2013845 | INBOUND | 10.240.220.47:4471 | 10.70.240.6 |
| 1902029 | INBOUND | 10.240.220.47:1575 | 10.240.21.119 |
| 1000096 | INBOUND | 10.240.220.47:80 | 10.240.30.8 |
| 894269 | INBOUND | 10.240.220.47:1575 | 10.240.11.29 |
| 690069 | INBOUND | 10.240.220.47:80 | 10.240.31.11 |
| 494429 | INBOUND | 10.240.220.47:443 | 10.240.32.211 |
| 322943 | INBOUND | 10.240.220.47:80 | 10.240.30.104 |
| 292112 | INBOUND | 10.240.220.47:3389 | 10.210.160.14 |
| 133239 | INBOUND | 10.240.220.47:1575 | 10.240.20.9 |
| 93444 | INBOUND | 10.240.220.47:3389 | 10.210.160.16 |
| 69369 | INBOUND | 10.240.220.47:3389 | 10.210.160.19 |

Outbound

| Count | Direction | Local IP | Remote IP : Port |
|---|---|---|---|
| 838112 | OUTBOUND | 10.240.220.47 | 10.70.240.6:135 |
| 800129 | OUTBOUND | 10.240.220.47 | 10.70.240.6:1026 |
| 783218 | OUTBOUND | 10.240.220.47 | 10.24.7.82:80 |
| 599411 | OUTBOUND | 10.240.220.47 | 10.70.240.6:88 |
| 583311 | OUTBOUND | 10.240.220.47 | 10.70.240.6:139 |
| 533121 | OUTBOUND | 10.240.220.47 | 10.70.240.6:1068 |
| 499321 | OUTBOUND | 10.240.220.47 | 10.24.1.37:53 |
| 354932 | OUTBOUND | 10.240.220.47 | 10.70.240.6:445 |
| 83811 | OUTBOUND | 10.240.220.47 | 10.24.1.38:53 |
| 43284 | OUTBOUND | 10.240.220.47 | 10.70.240.6:389 |
| 83811 | OUTBOUND | 10.240.220.47 | 10.24.1.39:53 |

## Network Spreadsheets

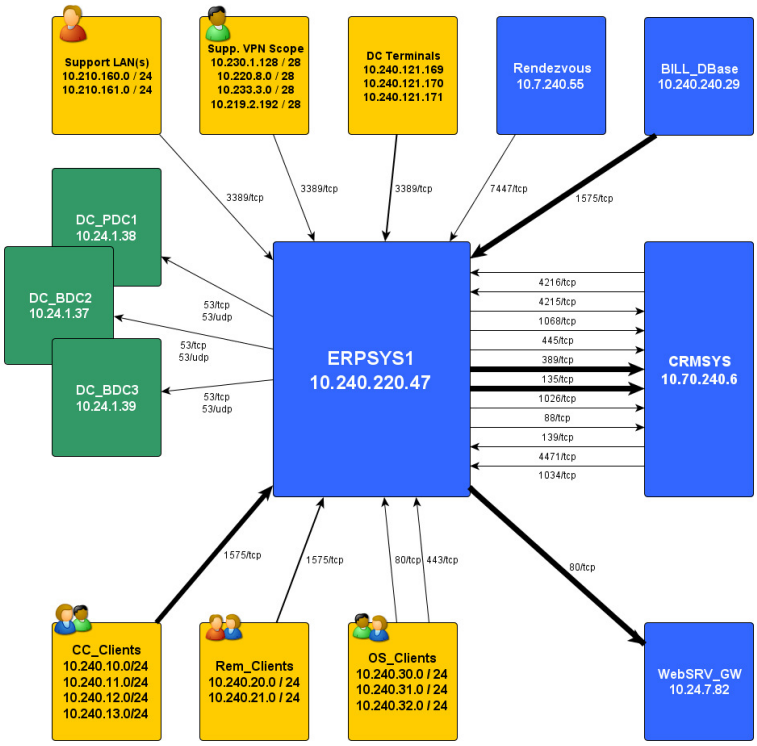
Alternatively this same information can be automatically imported into MS Excel or rendered as an Adobe Acrobat file - possibly for inclusion into a report.
In the case where the agent has been deployed to multiple servers, separate tabs can be used for each server.
In most cases a server/system's interconnections can be represented in as little as one side of A4 when printed, making review easy… never before has it been so simple to **see** a summary of your network traffic.

## Network Diagrams

If a visual representation is preferable then there is the option to output the data as a vector based network diagram.
This diagram (right) is an example of LANreveal output for a single host connectivity.

A few points to note:
1) Line thickness is proportional to traffic frequency (configurable)
2) Box size is proportional to traffic volume.
3) All ports are TCP unless stated otherwise.
4) Colours are used to represent different subnets/VLANs.

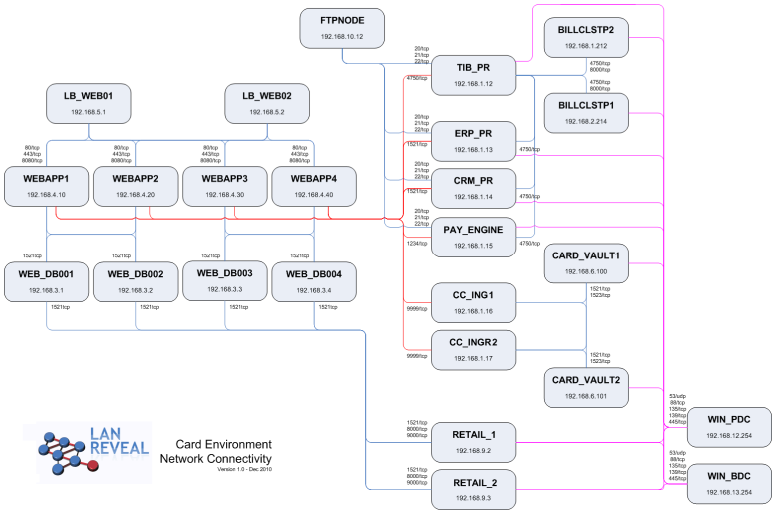
In this diagram (right), the server 'ERPSYS1' is the host of interest. The diagram shows all connectivity to and from this server. Using the diagramming features of LANreveal actually allows you to SEE the network interconnections.

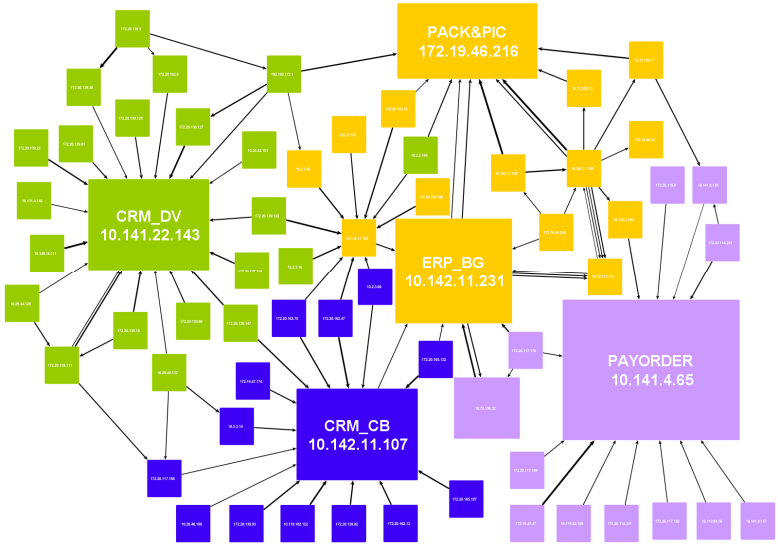



## Enterprise Diagrams

Alternatively, several hosts can be combined into one larger diagram showing all interconnections between key hosts and also any number of external systems.
These diagrams can be as simple or as complex as you require. To-date we've analysed systems with as few a 5 servers, or as many as 150.

The example (right) is a representation of an entire card processing environment for a major on-line retailer.

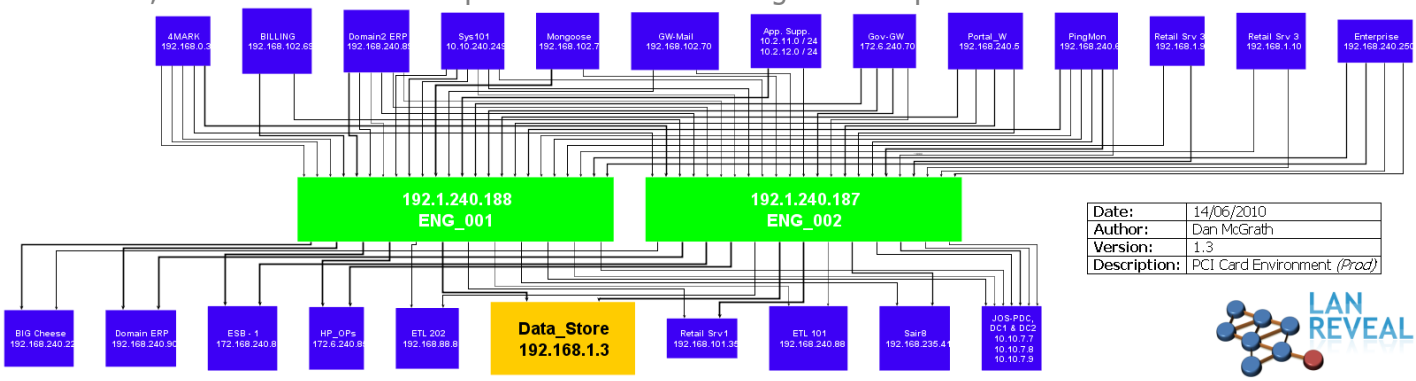



This diagram (left) depicts a number of key systems involved in a large warehousing / ERP system. Again colour is used to visually segment the diagram, and connecting lines of increased thickness are used to illustrate those connections that process high volumes of traffic.
This diagram was used to great effect as part of a large server virtualisation and data centre outsourcing project. The LANreveal agent was deployed on the 5 key warehouse servers, which revealed approximately 50 other dependant servers and facilitated the successful virtualisation and migration of the ERP system to an outsourced data centre.

## PCI:DSS Scoping

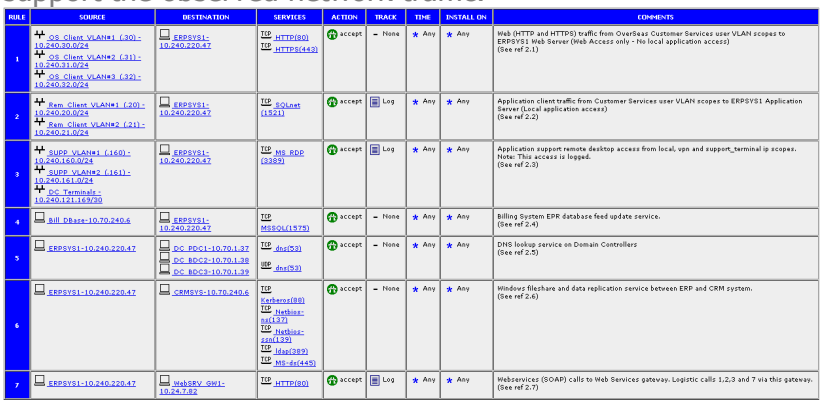
This diagram uses colour to great effect. Yellow is used to represent the in-scope (PCI) system, with Green used for all systems which directly connect to the in-scope (Yellow) system. Finally, Blue is used for all systems which interface with the Green. This provides a good starting point for a PCI scoping exercise. In this case, the different colours represent the different degrees of separation between hosts.

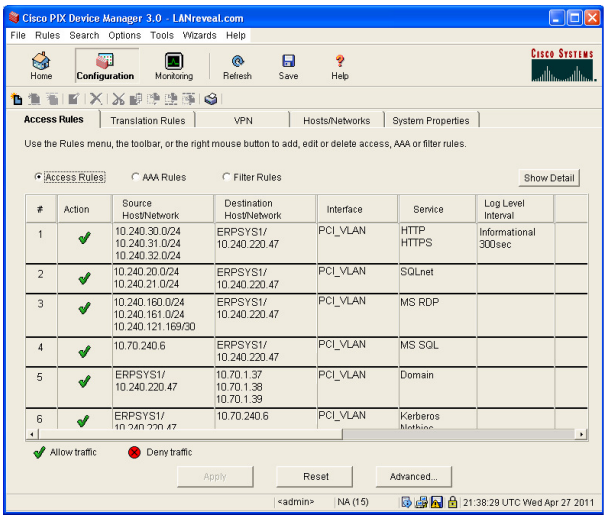



| | |
|---|---|
| Date: | 14/06/2010 |
| Author: | Dan McGrath |
| Version: | 1.3 |
| Description: | PCI Card Environment *(Prod)* |

## Firewall Configuration Files

Finally, we can take the information above, and use it to actually *(and automatically)* generate the firewall rule base to support the observed network traffic.




Firewall configurations can be generated and in most cases directly imported into both Cisco PIX/ASA and Checkpoint Firewall-1 (above)

## Contact

Thank you for your interest.

If you have any questions, please don't hesitate to get in touch:


**Website:** www.lanreveal.com
**Mail:** info@lanreveal.com
**Tel (mobile):** 07795 810880
**Tel (office):** 0117 9115412


**Evaluate Today!**

Request a free trial at:

**LANreveal.com/trial**

**ABOUT LANreveal**

LANreveal is the next generation network analysis, mapping and security assurance engine that really delivers. LANreveal provides a detailed view of network packet flow through your network based on what is actually happening in real-time. LANreveal offers the ability to accurately evaluate network paths to and from any host running the data collection agent. This evaluation is done off-line and does not involve any additional server processing overhead or introduction of additional packets onto the network.

Learn more @ **LANreveal.com**


Copyright © 2011 LANreveal. All rights reserved.
LANreveal and the LANreveal logo are trademarks of Activ8 Information Security Limited. All other registered or unregistered trademarks are the sole property of their respective owners