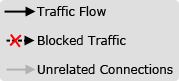
Network/Firewall Policy Interface Design

# Network Diagrams

The diagram describing the network is created by the user ahead of time by placing entities, connecting them with arrows and filling in policy details. Organizationally, there is a concept of a “zone,” which is merely a colored background for a specific group of entities and connections. It may be possible to derive this information from the type/sort information of a policy vocabulary file.The interface for drawing the diagrams has not been explored much yet.

# Arrows

Arrows are used to show the possible flow of traffic. When a specific model is being viewed, black arrows will show the actual traffic flow, while the irrelevant arrows are grayed out. When a path would have been taken (based on source and destination) but the packets were denied by a policy, the arrow is dashed and a red ‘x’ is drawn on it. The following key is used to describe this visualization.



# Entity Icons (to be changed)

## Computer/Host



This icon is used to represent a single computer with a single IP Address. It graphically represents a source or destination for traffic and does not have a policy or subcomponents.

## Server



This icon is used to represent a server. It is practically equivalent to the previous icon, but implies that it is used for different tasks.

## Group / External Network



This is used to represent a number of hosts with a collection of possible IP Addresses. An example of usage would be for representing the Internet or some external network.

## Firewall/Router



This represents an entity with policy rules, or one which contains subcomponents that implement policy rules.

# Policy Indicator Icons

These are used to describe the result of the policy rules for the specific traffic data. They appear near the entity which caused the specific result.

An entity which implements more than one policy (because of subcomponents, most likely) may have more than one icon appear near it.

## Permit

icon_accept.png

The packet is accepted by the policy.

## Deny

icon_deny.png

The packet is denied.

## Modify

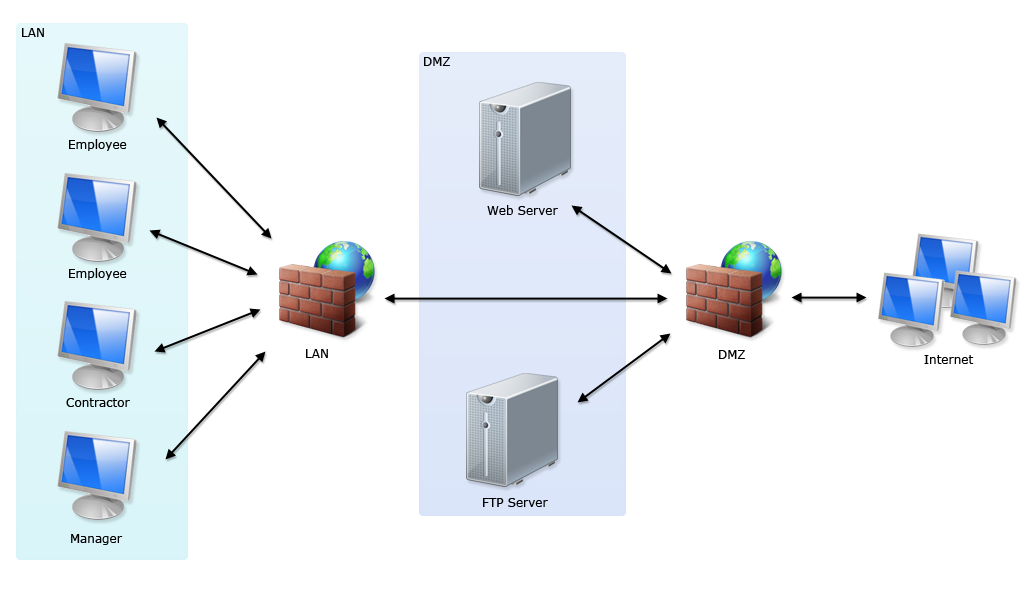
icon_modify.png

The packet has been modified in some way. Generally, the source or destination IP Address has been changed.

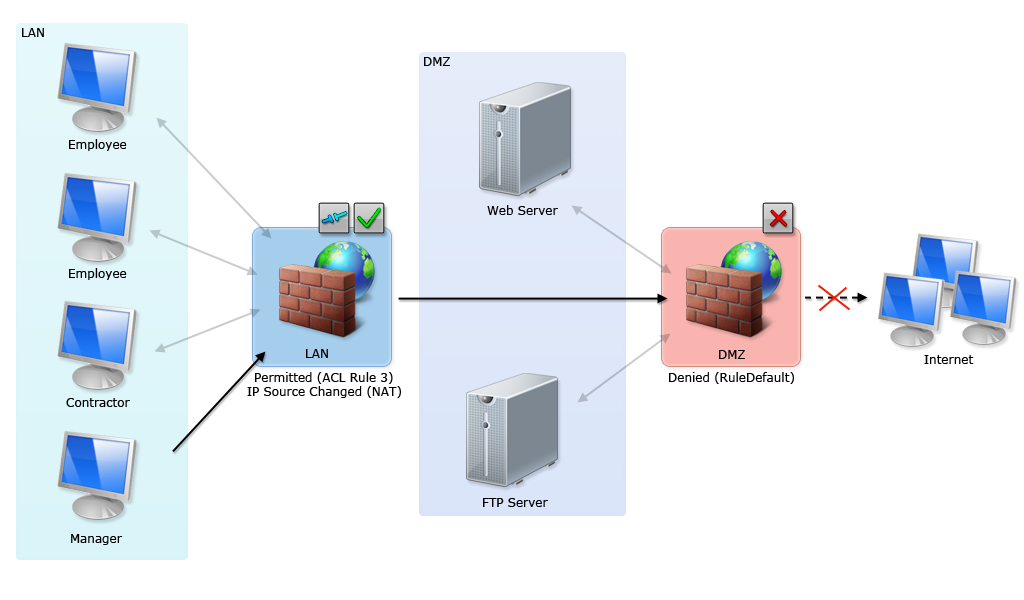
Other indicator icons could become necessary in the future, such as ones for routing behaviors or for other policy decisions.

# Examples

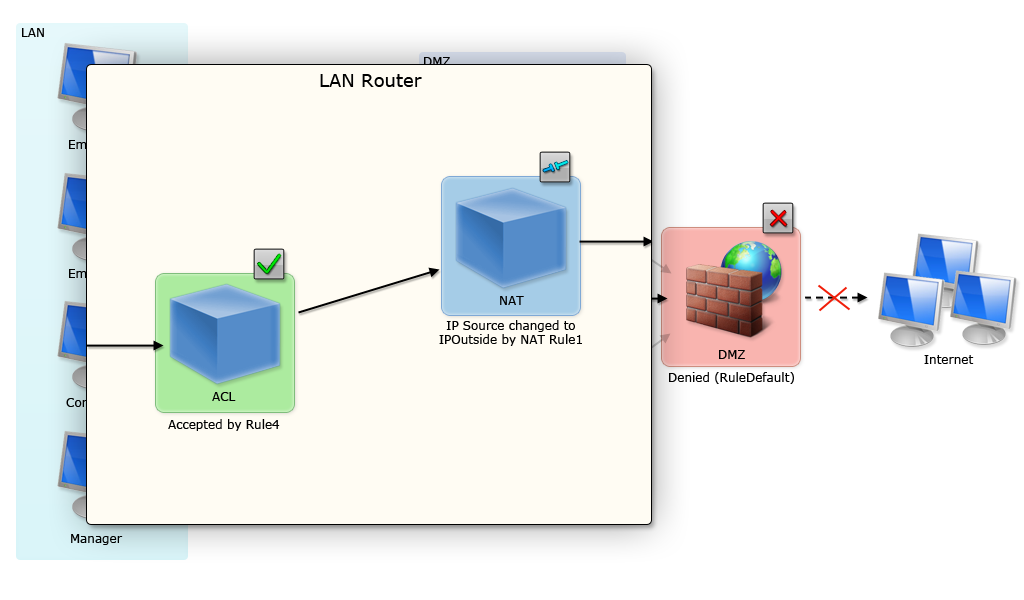
## Network Graph (created by the user)



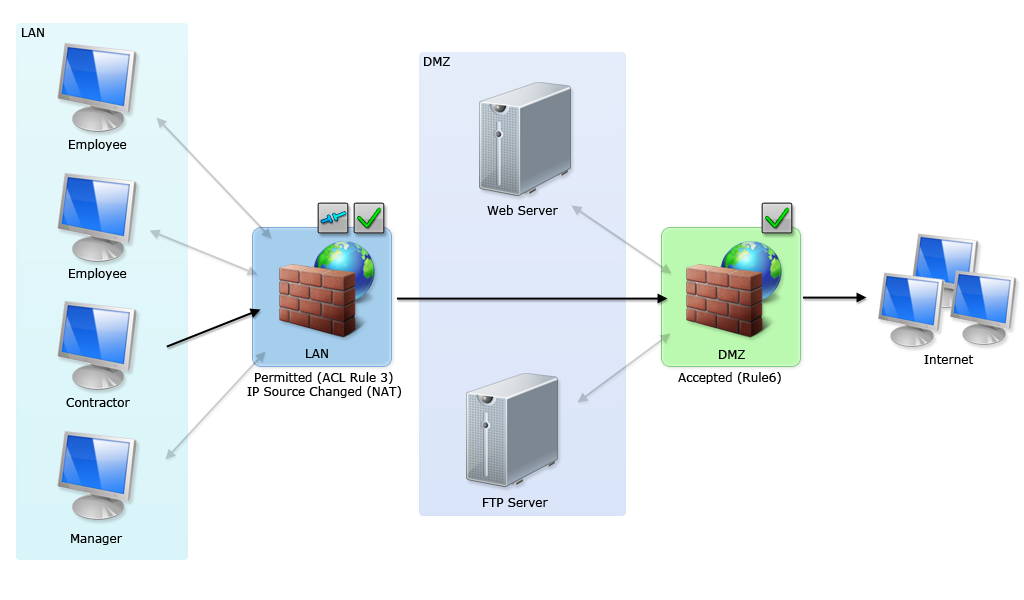
## Presentation Example – Manager unable to access the internet



## With subcomponents panel



## After the proposed “solution”



# User Interface Elements

## Diagram Window

The main window of the application contains the diagram. When no model/result is being viewed, this shows all connections and all entities as in the first example. When viewing a model, only the relevant arrows will be in black, others are grayed out. Additionally, important entities are highlighted as described in previous sections of this document.

## Query Field

The user can bring up a query window which allows him to write and execute a Margrave query. When the models have been retrieved, the query window is populated with the results. In addition, the main window is modified as in the above examples based on the current model.

## Model Selector

When multiple results are returned from Margrave, a group of controls appear which allow the user to switch between the models. For now, these consist of simply a left arrow, right arrow and text field with the model id.

## Packet Test

A potential tool in the interface would give users the ability to test if a packet with specific data about source, destination, port, etc. can reach its destination without being blocked by policy. This can be a useful shortcut instead of creating the query from scratch, and can be implemented with a representational interface. For example, the source and destination could be chosen by the user by clicking on the specific hosts, as opposed to typing out IP Addresses.

# Guidelines for Extending the Interface

## Possible Features

* A system for constructing queries other than typing them into a box.
* A way to organize models or name them intelligently (right now they have a mostly meaningless number associated with them)
* More icons for entities, just to reduce confusion and allow more expressive diagrams.

## Color Use

* Red means denied, disallowed, etc.
* Green means accepted, permitted, etc.
* Grey means disabled.
* Black is normal.

## Icons

Any information communicated through color must also have a descriptive icon. Color is not sufficiently universal and colorblindness is common.