



# **LCT**

## ( Logical Control Tool )

**Aim : Building advanced Firewall with Data Analytics capability using open-source components**

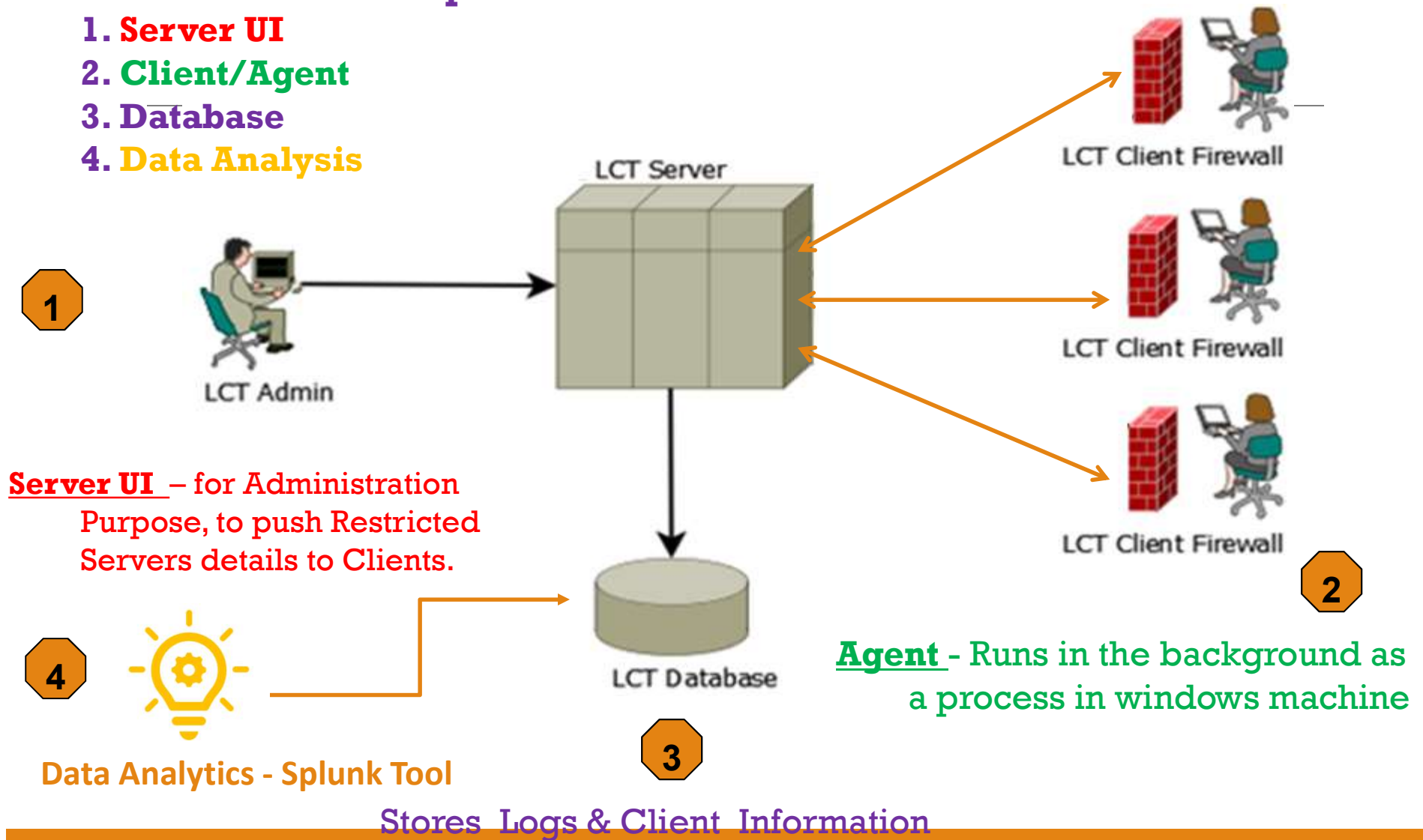
---

Srikanth Kumar Yekollu

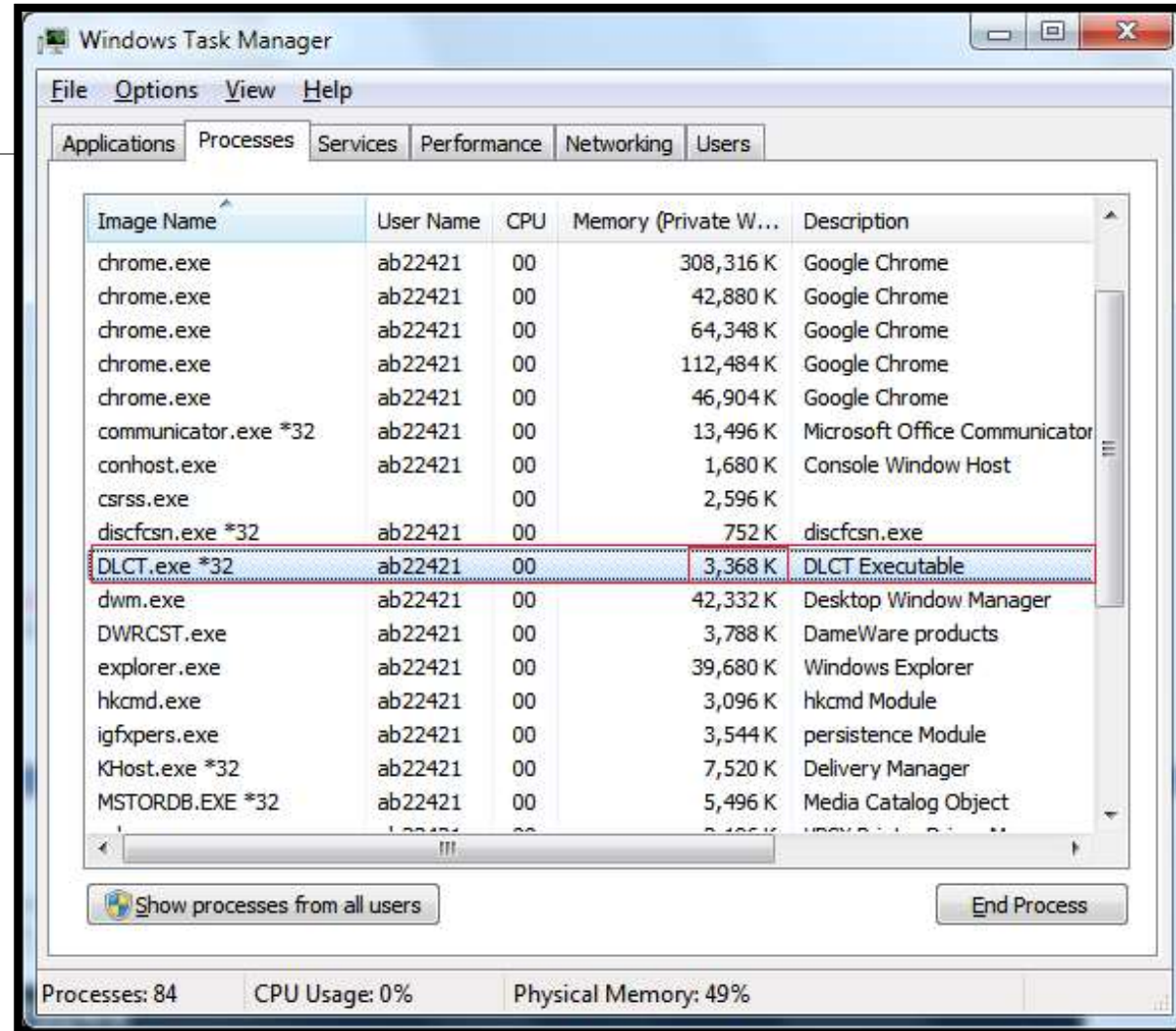
# Architecture :-

This tool has 4 Components

1. **Server UI**
2. **Client/Agent**
3. **Database**
4. **Data Analysis**



# Client:-



# IPFW:-

IPfirewall or ipfw is a open source FreeBSD IP packet filter and traffic accounting facility.

---

It is logically divided into 2 modules :

1. The Kernel Space Module
2. The User Space Module

The Kernel space module :

1. The Kernel space module is loaded into the network adapter as a service and acts as a packet filter.
2. Allowing or denying network traffic based on firewall rules defined by the admin.
3. It also allows for the logging of specific network traffic for analysis and reporting purposes.

# Installation :-

## The Kernel space module

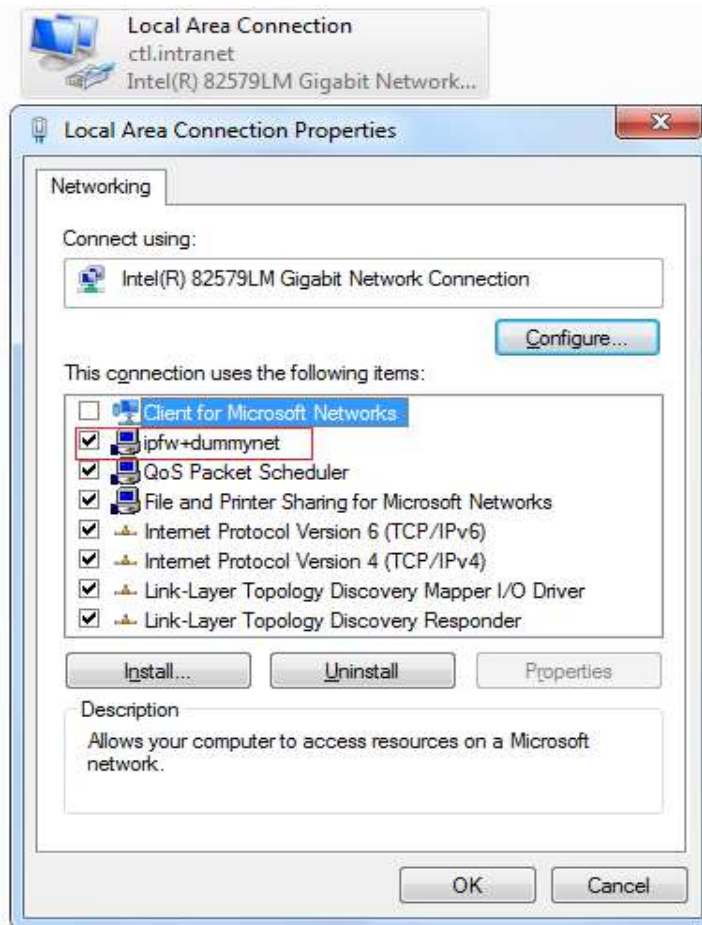


Fig: ipfw driver installation at network adapter

# IPFW

## The User Space Module :

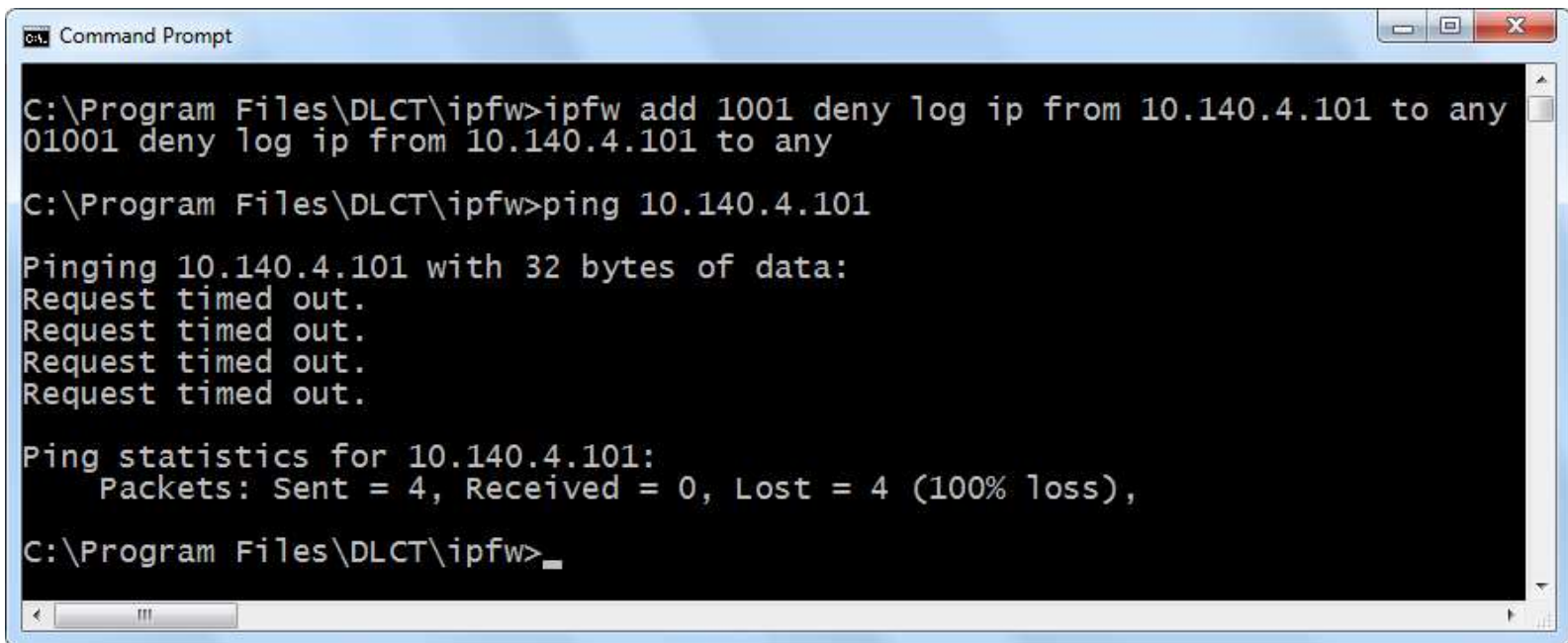
---

1. The user space module is an executable which communicates with the kernel space module via context switching.
2. Allows the addition/deletion of firewall rules programmatically.
3. We can apply all IPFW based command over it.

# IPFW

## The User Space Module :

---



```
C:\Program Files\DLCT\ipfw>ipfw add 1001 deny log ip from 10.140.4.101 to any
01001 deny log ip from 10.140.4.101 to any

C:\Program Files\DLCT\ipfw>ping 10.140.4.101

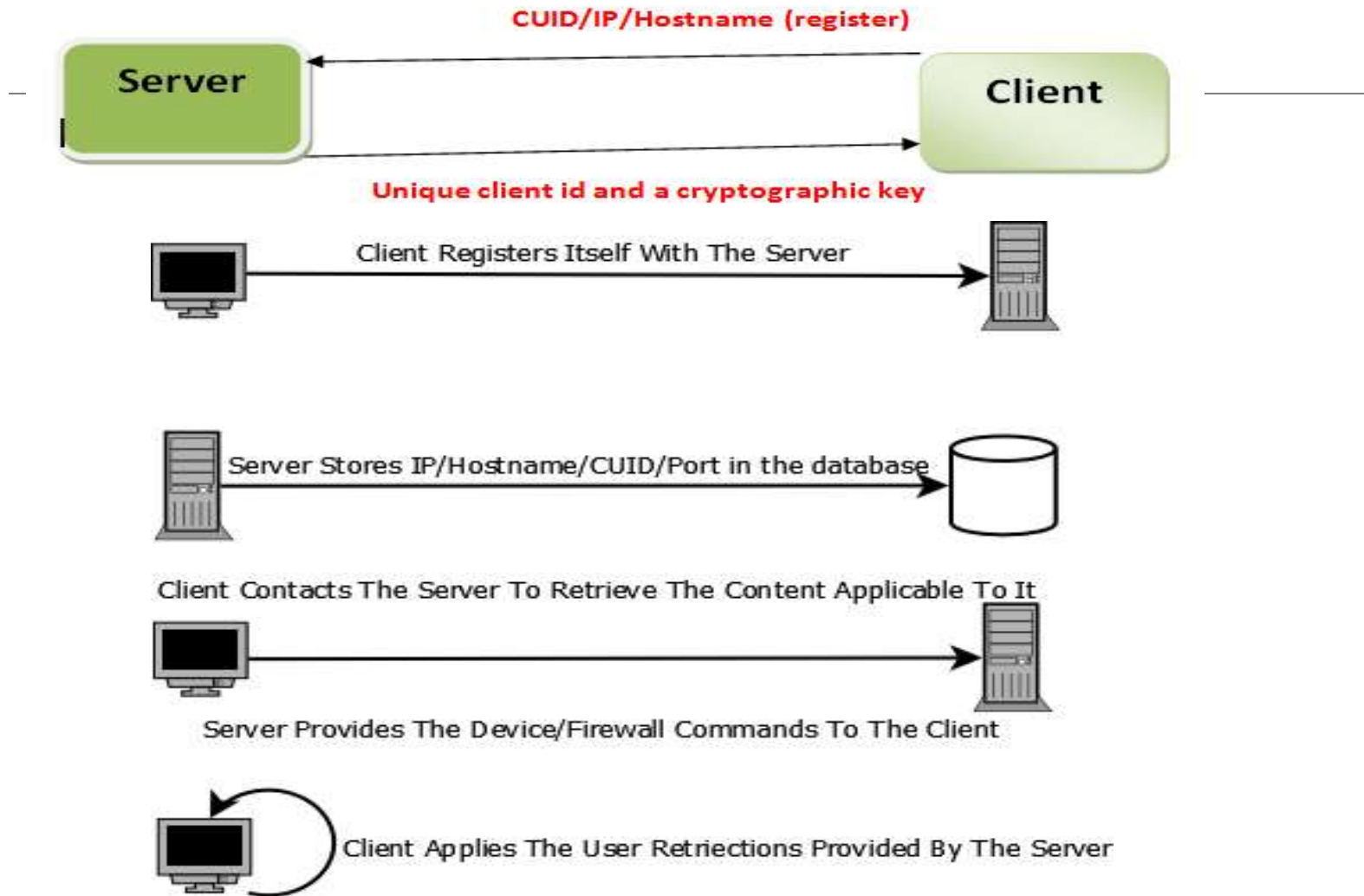
Pinging 10.140.4.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.140.4.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Program Files\DLCT\ipfw>
```

ip rule creation for IP blocking using command line

## How it Works ?





# Server UI

Rules

Profiles

Units

Groups

Bindings

Client Activity

Client Info

Client Content

Business Filters

Alert

Logout

Grouping bar (group by rule attributes)

	Number ^	Action ^	Protocol ^	Direction ^	Source Host ^	Source Not ^	Destination Host ^	Destination Not ^	Source Port ^	Destination Port ^
<input type="checkbox"/>	40	DENY	TCP	ANY	ANY	FALSE	10.140.18.12	FALSE		445
<input type="checkbox"/>	41	DENY	TCP	ANY	ANY	FALSE	10.140.18.12	FALSE		137
<input type="checkbox"/>	42	DENY	TCP	ANY	ANY	FALSE	10.140.18.12	FALSE	137	
<input type="checkbox"/>	43	DENY	UDP	ANY	ANY	FALSE	10.140.18.12	FALSE		138
<input type="checkbox"/>	44	DENY	UDP	ANY	ANY	FALSE	10.140.18.12	FALSE	138	
<input type="checkbox"/>	45	DENY	UDP	ANY	ANY	FALSE	10.140.18.12	FALSE		139
<input type="checkbox"/>	46	DENY	UDP	ANY	ANY	FALSE	10.140.18.12	FALSE	139	
<input type="checkbox"/>	47	DENY	IP	ANY	ANY	FALSE	10.140.18.12	FALSE		
<input type="checkbox"/>	51	ALLOW	TCP	ANY	ANY	FALSE	208.65.0.0/16	FALSE		
<input type="checkbox"/>	52	ALLOW	TCP	ANY	ANY	FALSE	208.117.0.0/16	FALSE		
<input type="checkbox"/>	100	ALLOW	IP	ANY	ANY	FALSE	ANY	FALSE	20	
<input type="checkbox"/>	101	ALLOW	ICMP	ANY	ANY	FALSE	ANY	FALSE		
<input type="checkbox"/>	105	ALLOW	IP	IN	ANY	FALSE	10.140.4.105	TRUE		
<input type="checkbox"/>	106	DENY	IP	ANY	10.140.6.183	FALSE	ANY	FALSE		
<input type="checkbox"/>	121	ALLOW	IP	ANY	ANY	FALSE	10.140.0.95	FALSE		
<input type="checkbox"/>	122	ALLOW	IP	ANY	ANY	FALSE	10.140.0.101	FALSE		

0

Page 0 of 0

20

rules per page

No rules to display

Content 1

Content 2

Content 3

Content 4

Number

Action

Protocol

Direction

Source Host

Source Not

Destination Host

Destination Not

Save

Reset

# Functionality:

1. Works as a Firewall and monitors Desktop Incoming & Outgoing packets.
- 
2. Provision to push Rules to desktops using either " IP or CUID or Machine Name".
  3. blocks the access to sensitive server when any attempt made by Non CR user .
  4. Logs the sensitive servers access attempts info & also alerts the Monitoring Team.
  5. Firewall Rules can be assigned to a group of desktops or Individual desktop level as well.
  6. Logs will be stored in Database for analysis and Reporting purpose using any big data tool- ex : Splunk )

# Benefits :-

1. Restricting non CR users accessing sensitive Servers/Applications
  2. Monitoring Tool
- 
3. Works for monitoring & blocking different connection types such as Remote Desktop, Browser, Database, any tool etc.
  4. Can disable Desktop drives as well( CD& USB )
  5. Light weight Application, hence no impact on the Client performance.
  6. Easy Administration.
  7. Built using Open source component.

# User Notification

