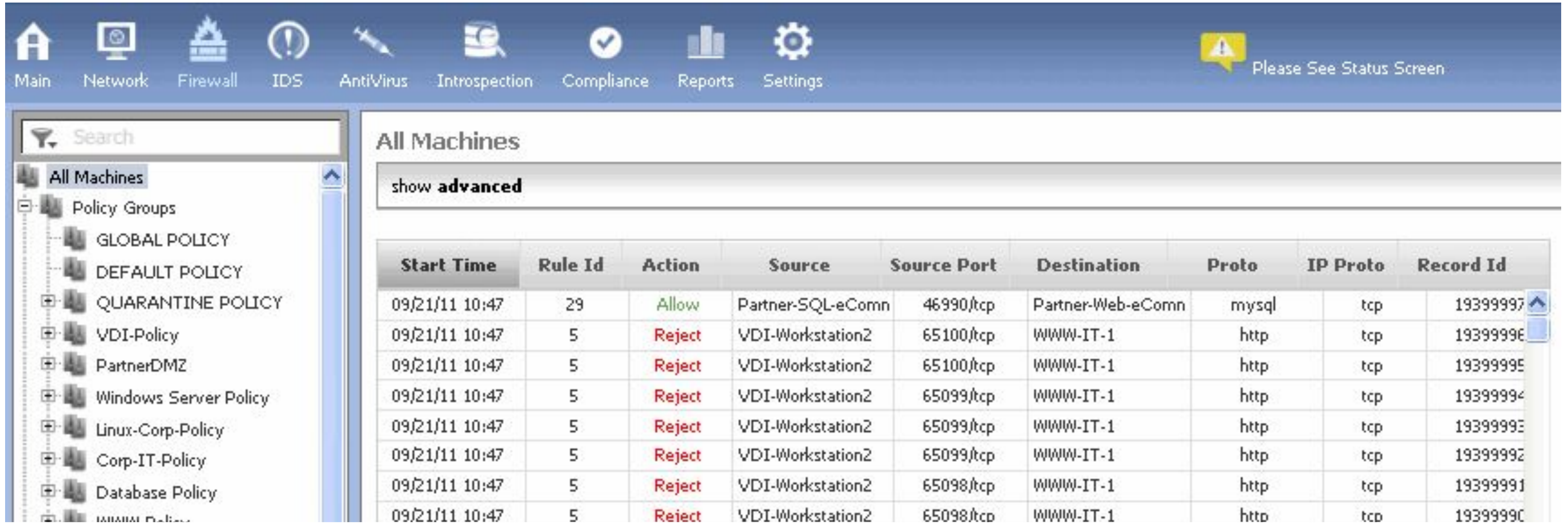




Ejemplo de REGEX II

Expresiones regulares

- Ejemplo: de un Firewalls de Juniper



The screenshot displays the Juniper Firewall configuration interface. The top navigation bar includes icons for Main, Network, Firewall, IDS, AntiVirus, Introspection, Compliance, Reports, and Settings. A status message on the right says "Please See Status Screen".

On the left, a sidebar shows a tree view of policy groups under "All Machines". The tree includes:

- Policy Groups
 - GLOBAL POLICY
 - DEFAULT POLICY
 - QUARANTINE POLICY
 - VDI-Policy
 - PartnerDMZ
 - Windows Server Policy
 - Linux-Corp-Policy
 - Corp-IT-Policy
 - Database Policy

The main area, titled "All Machines", shows a "show advanced" button and a table of traffic logs.

| Start Time | Rule Id | Action | Source | Source Port | Destination | Proto | IP Proto | Record Id |
|----------------|---------|--------|-------------------|-------------|-------------------|-------|----------|-----------|
| 09/21/11 10:47 | 29 | Allow | Partner-SQL-eComn | 46990/tcp | Partner-Web-eComn | mysql | tcp | 19399997 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65100/tcp | WWW-IT-1 | http | tcp | 19399996 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65100/tcp | WWW-IT-1 | http | tcp | 19399995 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65099/tcp | WWW-IT-1 | http | tcp | 19399994 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65099/tcp | WWW-IT-1 | http | tcp | 19399993 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65099/tcp | WWW-IT-1 | http | tcp | 19399992 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65098/tcp | WWW-IT-1 | http | tcp | 19399991 |
| 09/21/11 10:47 | 5 | Reject | VDI-Workstation2 | 65098/tcp | WWW-IT-1 | http | tcp | 19399990 |

Expresiones regulares

- Ejemplo: Log del FW de Juniper visto anteriormente:

- **09/21/11 10:47 29 Allow Partner-SQL-eComm 46990 tcp Partner-Web-eComm mysql 19999**

- Separador de campos: ESPACIO (\s)

- Mapeo de campos:

- Fecha + Hora: 09/21/11 10:47
- Numero regla: 29
- Acción realizada: Allow o Reject
- Origen: Partner-SQL-eComm
- Puerto Origen: 46990
- Destino: Partner-Web-eComm
- Protocolo: Mysql
- IP protocolo: tcp
- RecordID: 19999

- Expresión Regular: ¿?



Expresiones regulares

- Ejemplo: Log del FW de Juniper visto anteriormente:

- **09/21/11 10:47 29 Allow Partner-SQL-eComm 46990 tcp Partner-Web-eComm mysql 19999**

- Separador de campos: ESPACIO (\s)

- Mapeo de campos:

- Fecha + Hora: 09/21/11 10:47
- Numero regla: 29
- Acción realizada: Allow o Deny
- Origen: Partner-SQL-eComm
- Puerto Origen: 46990
- Destino: Partner-Web-eComm
- Protocolo: Mysql
- IP protocolo: tcp
- RecordID: 19999

- Expresión Regular:

- `(.*)\s(.*)\s(.*)\s(.*)\s(.*)\s(.*)\s(.*)`
- `^(\d{2}\d{2}\d{2})\s(\d{2}:\d{2})\s(\d+)\s(Allow|Deny)\s(.*)\s(\d+)\s(tcp|udp)\s(\d+)\s(\d+)`