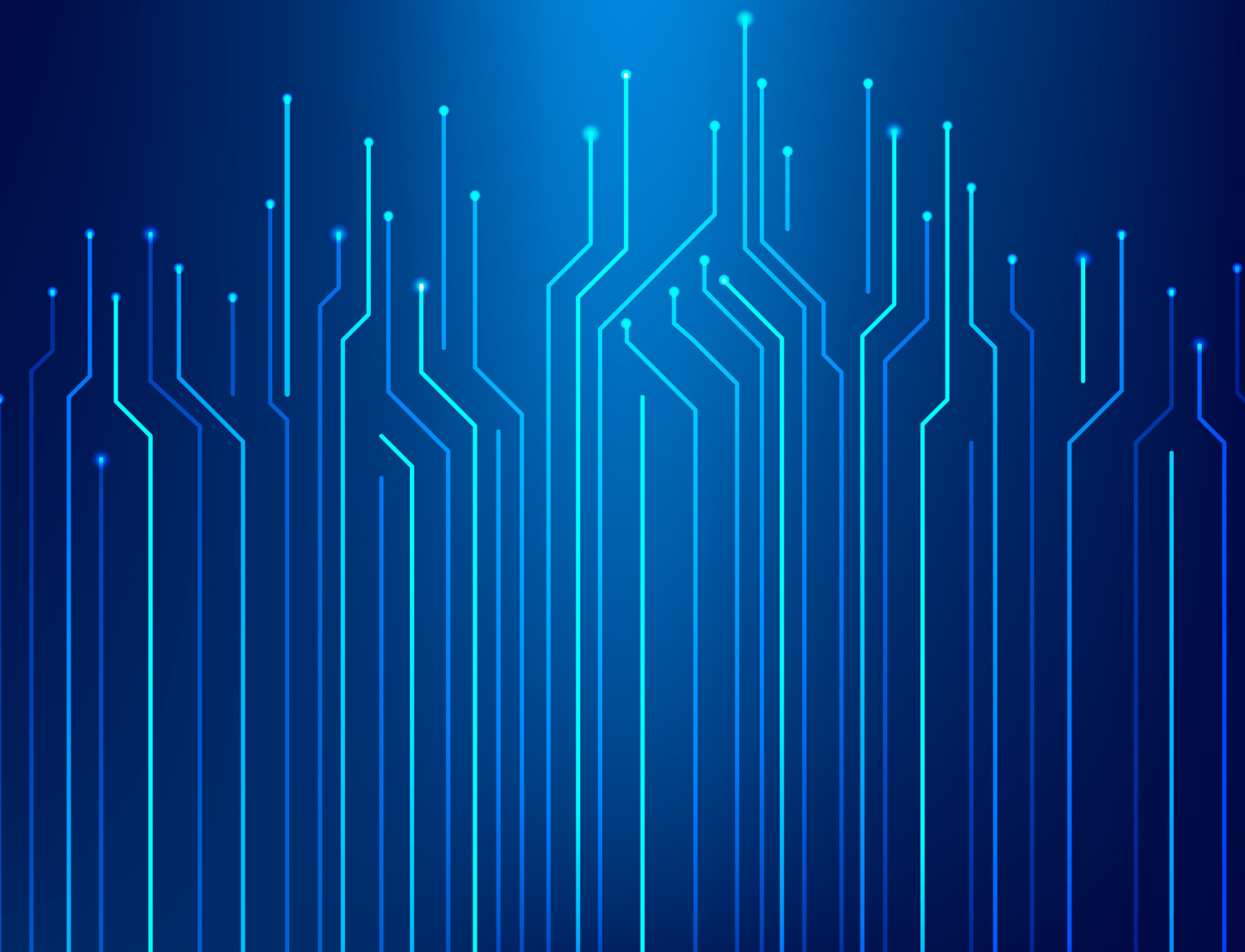

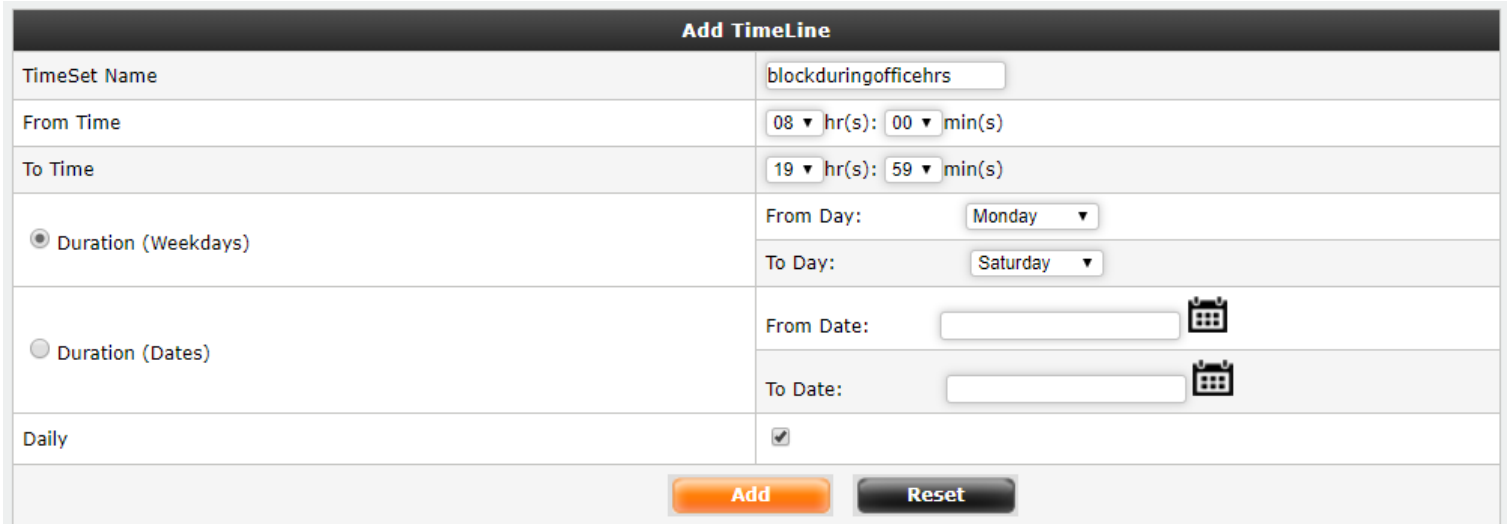




How to block/allow URL or application for a period of time using time based schedule



How to block/allow URL or application for a period of time using time based schedule

To add a new timeline, Go to Definitions -> Time Schedule and click on  icon. The following screen appears:



| Add TimeLine | |
|---|--|
| TimeSet Name | blockduringofficehrs |
| From Time | 08 hr(s): 00 min(s) |
| To Time | 19 hr(s): 59 min(s) |
| <input checked="" type="radio"/> Duration (Weekdays) | From Day: Monday To Day: Saturday |
| <input type="radio"/> Duration (Dates) | From Date: <input type="text"/>  To Date: <input type="text"/>  |
| Daily | <input checked="" type="checkbox"/> |
| <input type="button" value="Add"/> <input type="button" value="Reset"/> | |

This section allows to add new Time Set.

TimeSet Name: Name of time set.

From Time: You can select hours and minutes.

To Time: You can select hours and minutes.

Either select Duration (Weekdays):

From Day: You can select day of week for **From day**.

To Day: You can select day of week for **To day**.

Or select Duration (Dates):

From Date: You can select From Date to create TimeSet based on specific date.

To Date: You can select To Date to create TimeSet based on specific date.

Daily: If this option is selected, Time will be considered on daily basis.

| | | | | | | |
|----------------------|--------|-------|----------|-------|---|---|
| blockduringofficehrs | Monday | 08:00 | Saturday | 19:59 | ✓ |    |
|----------------------|--------|-------|----------|-------|---|---|

Now go to the URL filtering tab by clicking on Browsing -> Policy -> URL Filter Policy and add the details like time-stamp and assign it to a URL filtering policy template.

URL Filter Policy | URL QoS Policy | Exception Sites

Add URL Filter Policy Template


Policy Name:

Parent Policy Name:

URL Filter Policy

Default Action:

Enable Strict Search: Yes No


Categories to Block: 


White List URLs:

Black List URLs:

Download Policy



Default Action:

Mime Types to Block: 

File Extension Types to Block: 

File Size Download Limit to Block: Alert if limit exceeds

Bypass Download Policy Urls:

| | | | | |
|------------------|---|-------|-------|---|
| blockinofficehrs | - | block | allow |    |
|------------------|---|-------|-------|---|

Now go to Firewall -> Policies -> Rules and add the URL filtering template and the time-stamp to the firewall policy.

The screenshot shows the configuration interface for a Firewall Policy. At the top, there are tabs for 'Rules', 'Port Forwarding', 'DoS Settings', 'MAC Binding', 'MAC Filtering', and 'Install Policies'. The 'Rules' tab is selected.

Action and Logging

| | |
|---------------|------------------------|
| Action | Accept ▼ |
| Time Schedule | blockduringofficehrs ▼ |
| Status | Active ▼ |
| Log | Yes ▼ |
| Comment | <input type="text"/> |

Hide Advanced Options

Security Policies

| | |
|--|---|
| Application filter Policy | Please Select ▼ |
| Data Leak Prevention(DLP) Policy | Please Select ▼ |
| Intrusion Prevention System(IPS) Policy | Please Select ▼ |
| Url filter Policy | blockinofficehrs ▼ <input type="checkbox"/> Proceed |
| SSL Deep Inspect (Applicable for All Https Urls) | <input checked="" type="checkbox"/> |
| Bypass DoS Settings | <input type="checkbox"/> |
| Bypass Stateful Inspection | <input type="checkbox"/> |
| Bypass IPS Policy | <input type="checkbox"/> |

- **Time Schedule:** Select the schedule to be applied for this rule. New Time Schedule object can be added in the Definition -> Time Schedule -> TimeSet Option and then use it here.
- **URL filter Policy:** Select the URL filtering policy you would like to apply to this rule. You can add new URL filter policy from Browsing -> Policy -> URL Filter Policy.
- **SSL Deep Inspect (Applicable for All Https URLs):** Select this option if you wish to deep inspect SSL traffic, mainly used to for https filtering. If you have enabled DLP feature then you need to check SSL deep inspect check box to enable DLP for HTTPS (SSL) traffic.

| No. | IP Version | Direction | Source | Destination | Service | UserSense | Policies | Action | Schedule | QoS | Tasks |
|-----|------------|------------|--------------|-------------|---------|-----------|---|--------|--------------------------------------|------------------------|-------|
| 1 | IPv4 | Any To Any | CloudNetwork | internet | Any | - | Url Filter Policy: blockinofficehrs SSL Deep Inspect: on | accept | blockduringofficehrs | Route Failover: GLOBAL | |
| 2 | IPv4 | Any To Any | CloudNetwork | internet | Any | - | Url Filter Policy: Open SSL Deep Inspect: on | accept | AllTime | Route Failover: GLOBAL | |

NOTE: Make sure the priority of this policy is above the current browsing policy to make it effective.

Thus you have successfully configured a policy to block/allow URL or application for a period of time using time base schedule.