Security

Flow

- Firewall
- Authentication
- Authorization

Firewall

- <u>Listener</u> to kernel.request
- <u>Firewall map configuration</u>
- <u>Security false Firewall</u>

Authentication

Firewall is a listener to "kernel.request" event

Flow

- Iterate over firewalls to match the url
- Match
  - Create an Anonymous Token
  - Iterate over authenticators (authentication listeners)
    - Find credentials at the Request
      - Found
        - Authenticate
      - Not found
        - Send to default Entry Point to fill the Request
- Not Match
  - Token is NULL

Token

- Implements TokenInterface
- Can be changed during request
- Stored at TokenStorage

User Provider

- Implements UserProviderInterface
- Required for authentication

Entry Point

Instruction to Client to authenticate the User.

For example:

- Display Login Form

- Headers

- Status Code

- Etc.

Implements AuthenticationEntryPointInterface

Usually returns RedirectResponse

Authenticators

- AuthenticationManagerInterface
- AuthenticationProviderInterface
- Login Form
- WSSE
- OAuth
- LDAP
- Remember Me
- etc.

Authorization

- [AccessDecissionManagerInterface](#)
- Strategies
  - affirmative (default) - grant if one voter granting
  - consensus - grant if more granting than denying
  - unanimous - grant if no one denying (Used By ORO)

Permissions Check

Bad

- token->getUser() !== null
- If ($user->isAdmin() || $user->hasRole(...

Good

- AuthorizationChecker

```php
if (!$this->authorizationChecker->isGranted('EDIT', $contact)) {
    throw new AccessDeniedException();
}
```

Permission Attributes

Roles
- ROLE_ADMIN

Special roles
- IS_AUTHENTICATED_FULLY
- IS_AUTHENTICATED_REMEMBERED
- IS_AUTHENTICATED_ANONYMOUSLY

Any other string identifiers
- VIEW, EDIT, DELETE
- oro_contact_view

Security Voters

- VoterInterface
- AclVoter
- RoleVoter
- ExpressionVoter
- Custom Attribute Voters
- AbstractEntityVoter

ACL at Oro

- Custom Role based implementation
- Default Permissions loaded in <u>Migrations</u>
- Permissions Managed from UI
- <u>AclHelper</u> for Queries

Debug

- debug:config security
- config:dump security
- [Good place to set the breakpoint](#)