

Sprint Planning Meeting Minutes:

Attendees: Nikolas Tsalikis, Anthony Pacheco, Lucca Pinto, Federico Marrero, Katherine Cruz

Start time: 7:45 p.m.

End time: 10:45 p.m.

After discussion, the velocity of the team was estimated to be - Two weeks

The product owner chose the following user stories to be done during the next sprint. They are ordered based on their priority.

- 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
- 2- Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.
- 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
- 4 - Start the process of documentation for all our configurations.
- 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
- 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)

The team members indicated their willingness to work on the following user stories.

- Nikolas Tsalikis
 - 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
 - 2 - Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.
 - 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
 - 4 - Start the process of documentation for all our configurations.
 - 5 - Review firewall and routing changes to ensure they align with established security standards.
 - 6 - Coordinate testing results across the team and resolve any integration concerns.
 - 7 - Oversee documentation accuracy and consistency across all configuration changes.
 - 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
 - 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)
 - 10 - Consider adding another certificate authority to allow clients to authenticate against different trusted CAs.

- Anthony Pacheco
 - 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
 - 2 - Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.
 - 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
 - 4 - Start the process of documentation for all our configurations.
 - 5 - Perform validation testing on firewall and split tunneling configurations.
 - 6 - Compare database performance impacts between SQLite and alternative options.
 - 7 - Assist in documenting test results and configuration findings.
 - 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
 - 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)
 - 10 - Consider adding another certificate authority to allow clients to authenticate against different trusted CAs.
- Lucca Pinto
 - 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
 - 2 - Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.
 - 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
 - 4 - Start the process of documentation for all our configurations.
 - 5 - Review how firewall and routing changes may impact UI behavior or user feedback.
 - 6 - Assist with documenting configuration steps that affect the client-side experience.
 - 7 - Validate that configuration changes do not negatively affect usability.
 - 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
 - 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)
 - 10 - Consider adding another certificate authority to allow clients to authenticate against different trusted CAs.
- Federico Marrero
 - 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
 - 2 - Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.

- 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
- 4 - Start the process of documentation for all our configurations.
- 5 - Ensure firewall and split tunneling configurations align with cryptographic and security best practices.
- 6 - Review database usage from a security and performance standpoint.
- 7 - Document security-related configuration decisions and justifications.
- 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
- 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)
- 10 - Consider adding another certificate authority to allow clients to authenticate against different trusted CAs.
- Katherine Cruz
 - 1 - Configure the outbound/inbound rules through the UFW firewall used for our VPN server.
 - 2 - Test split tunneling and determine if this is optimal instead of setting a full tunnel for internet traffic.
 - 3 - Determine if a database can be used in our VPN's use case and also determine if we want to keep the default of SQLite.
 - 4 - Start the process of documentation for all our configurations.
 - 5 - Organize and structure documentation for clarity and consistency.
 - 6 - Review configuration documentation for completeness and accuracy.
 - 7 - Assist with summarizing findings and decisions made during the sprint.
 - 8 - Update the Certificate Revocation List (CRL) to keep track of verified clients and remove certificates that have been compromised.
 - 9 - Start filling out the client profiles with the information needed (CA certificate, signed client certificate, and the client private key)
 - 10 - Consider adding another certificate authority to allow clients to authenticate against different trusted CAs.