Threat Modeling Report

Created on 9/11/2023 10:38:43 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	23
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	23
Total Migrated	0

Diagram: Diagram 1

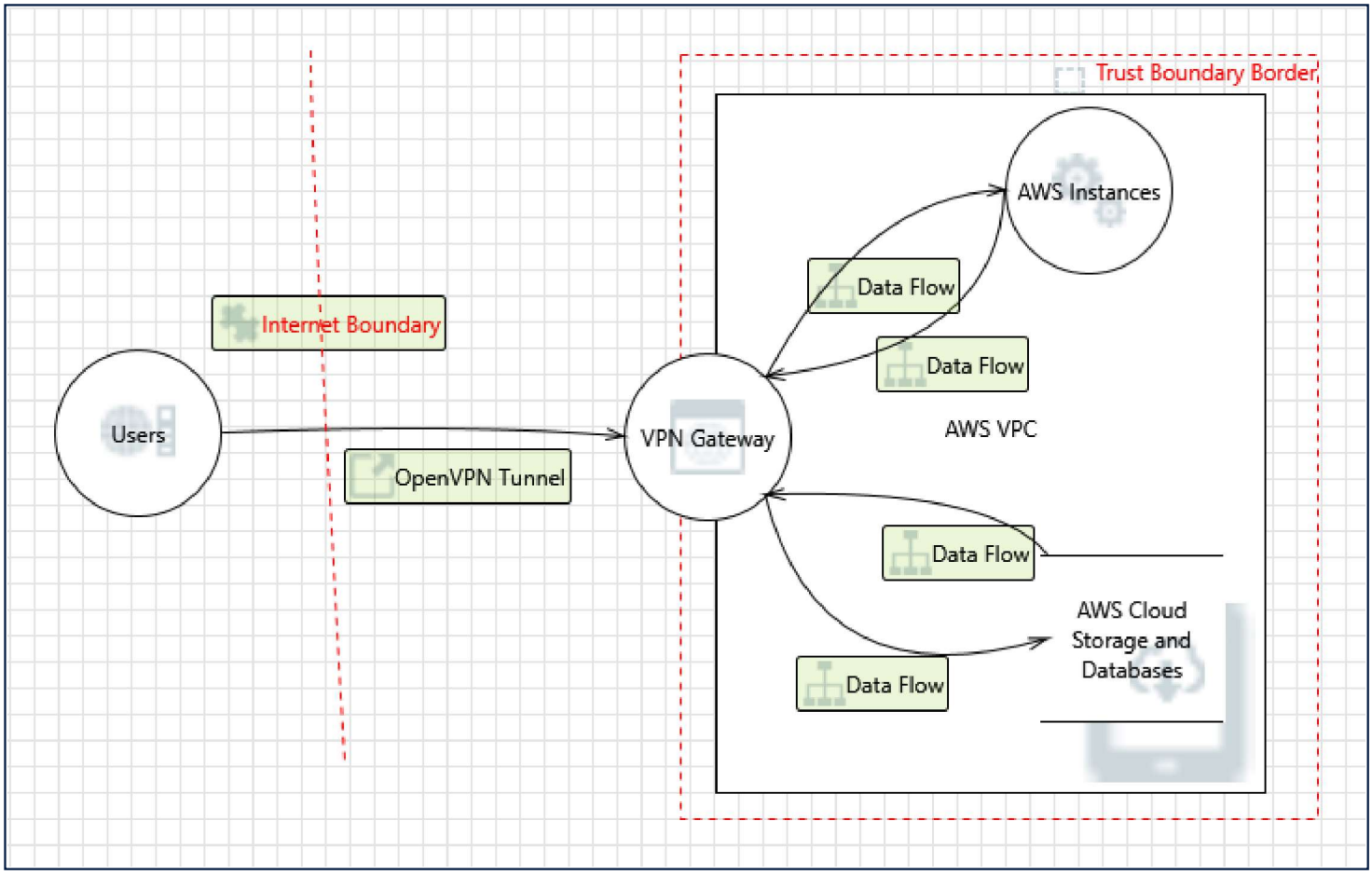
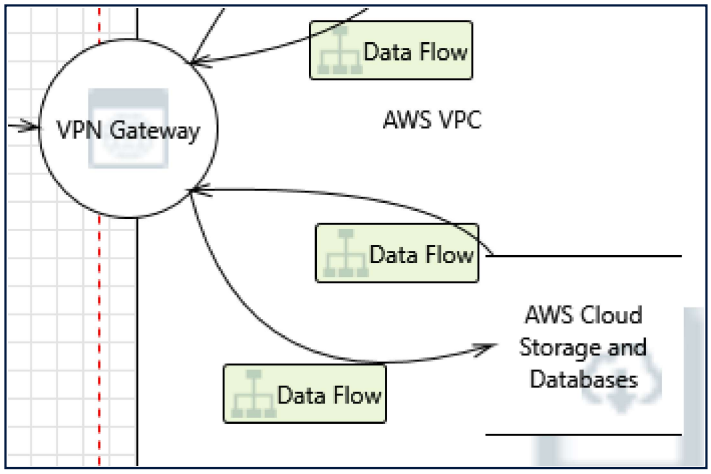


Diagram 1 Diagram Summary:

Not Started	23
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	23
Total Migrated	0

Interaction: Data Flow



1. Potential Excessive Resource Consumption for VPN Gateway or AWS Cloud Storage and Databases [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does VPN Gateway or AWS Cloud Storage and Databases take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: <no mitigation provided>

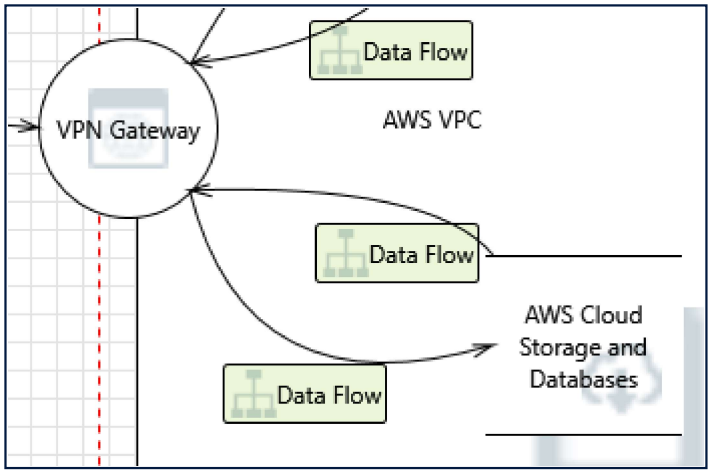
2. Spoofing of Destination Data Store AWS Cloud Storage and Databases [State: Not Started] [Priority: High]

Category: Spoofing

Description: AWS Cloud Storage and Databases may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of AWS Cloud Storage and Databases. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

Interaction: Data Flow



3. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of AWS Cloud Storage and Databases can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: <no mitigation provided>

4. Persistent Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'VPN Gateway' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'AWS Cloud Storage and Databases' inputs and output.

Justification: <no mitigation provided>

5. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'VPN Gateway' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: <no mitigation provided>

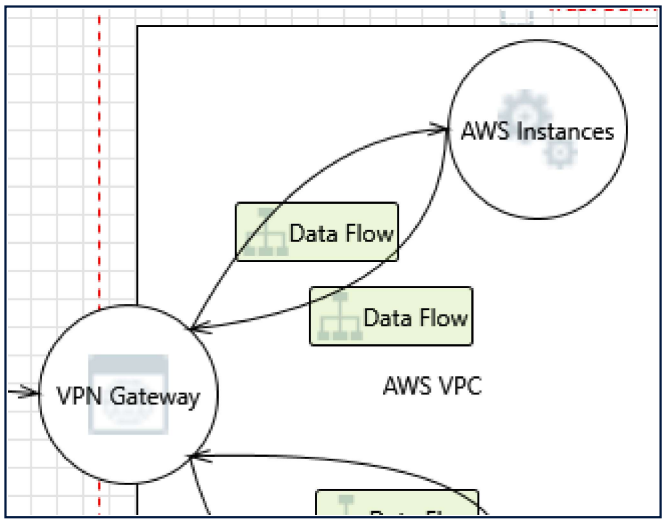
6. Spoofing of Source Data Store AWS Cloud Storage and Databases [State: Not Started] [Priority: High]

Category: Spoofing

Description: AWS Cloud Storage and Databases may be spoofed by an attacker and this may lead to incorrect data delivered to VPN Gateway. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

Interaction: Data Flow



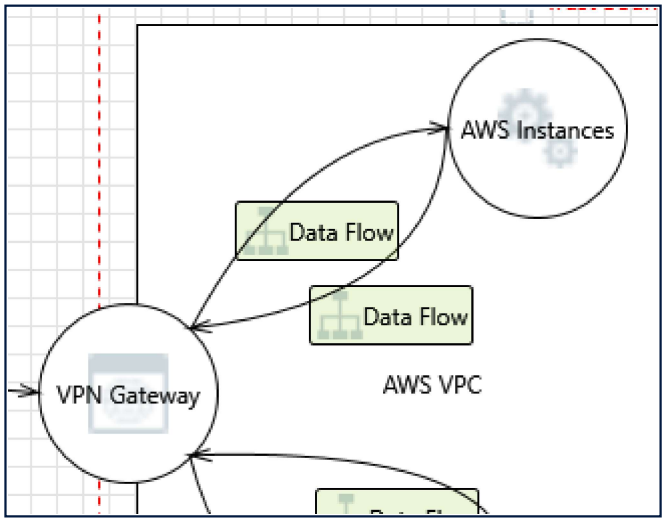
7. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: AWS Instances may be able to impersonate the context of VPN Gateway in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: Data Flow



8. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: VPN Gateway may be able to impersonate the context of AWS Instances in order to gain additional privilege.

Justification: <no mitigation provided>

9. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'VPN Gateway' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: <no mitigation provided>

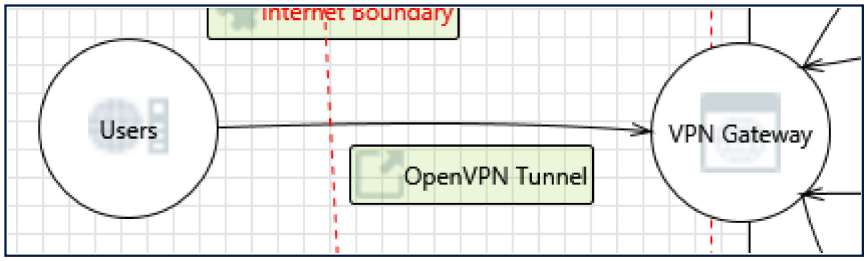
10. AWS Instances Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering

Description: If AWS Instances is given access to memory, such as shared memory or pointers, or is given the ability to control what VPN Gateway executes (for example, passing back a function pointer.), then AWS Instances can tamper with VPN Gateway. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: <no mitigation provided>

Interaction: OpenVPN Tunnel



11. Users Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering

Description: If Users is given access to memory, such as shared memory or pointers, or is given the ability to control what VPN Gateway executes (for example, passing back a function pointer.), then Users can tamper with VPN Gateway. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: <no mitigation provided>

12. Potential Lack of Input Validation for VPN Gateway [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across OpenVPN Tunnel may be tampered with by an attacker. This may lead to a denial of service attack against VPN Gateway or an elevation of privilege attack against VPN Gateway or an information disclosure by VPN Gateway. Failure to verify that input is as

expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: <no mitigation provided>

13. Spoofing the Users Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Users may be spoofed by an attacker and this may lead to unauthorized access to VPN Gateway. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

14. Authenticated Data Flow Compromised [State: Not Started] [Priority: High]

Category: Tampering

Description: An attacker can read or modify data transmitted over an authenticated dataflow.

Justification: <no mitigation provided>

15. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'VPN Gateway' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: <no mitigation provided>

16. Potential Data Repudiation by VPN Gateway [State: Not Started] [Priority: High]

Category: Repudiation

Description: VPN Gateway claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: <no mitigation provided>

17. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Data flowing across OpenVPN Tunnel may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: <no mitigation provided>

18. Potential Process Crash or Stop for VPN Gateway [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: VPN Gateway crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: <no mitigation provided>

19. Data Flow OpenVPN Tunnel Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: <no mitigation provided>

20. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: VPN Gateway may be able to impersonate the context of Users in order to gain additional privilege.
Justification: <no mitigation provided>

21. VPN Gateway May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Users may be able to remotely execute code for VPN Gateway.
Justification: <no mitigation provided>

22. Elevation by Changing the Execution Flow in VPN Gateway [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into VPN Gateway in order to change the flow of program execution within VPN Gateway to the attacker's choosing.
Justification: <no mitigation provided>

23. Cross Site Request Forgery [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry

the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: <no mitigation provided>