Threat Modeling Report

Created on 11/30/2025 9:03:16 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	26
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	13
Total	39
Total Migrated	0

Diagram: Diagram 1

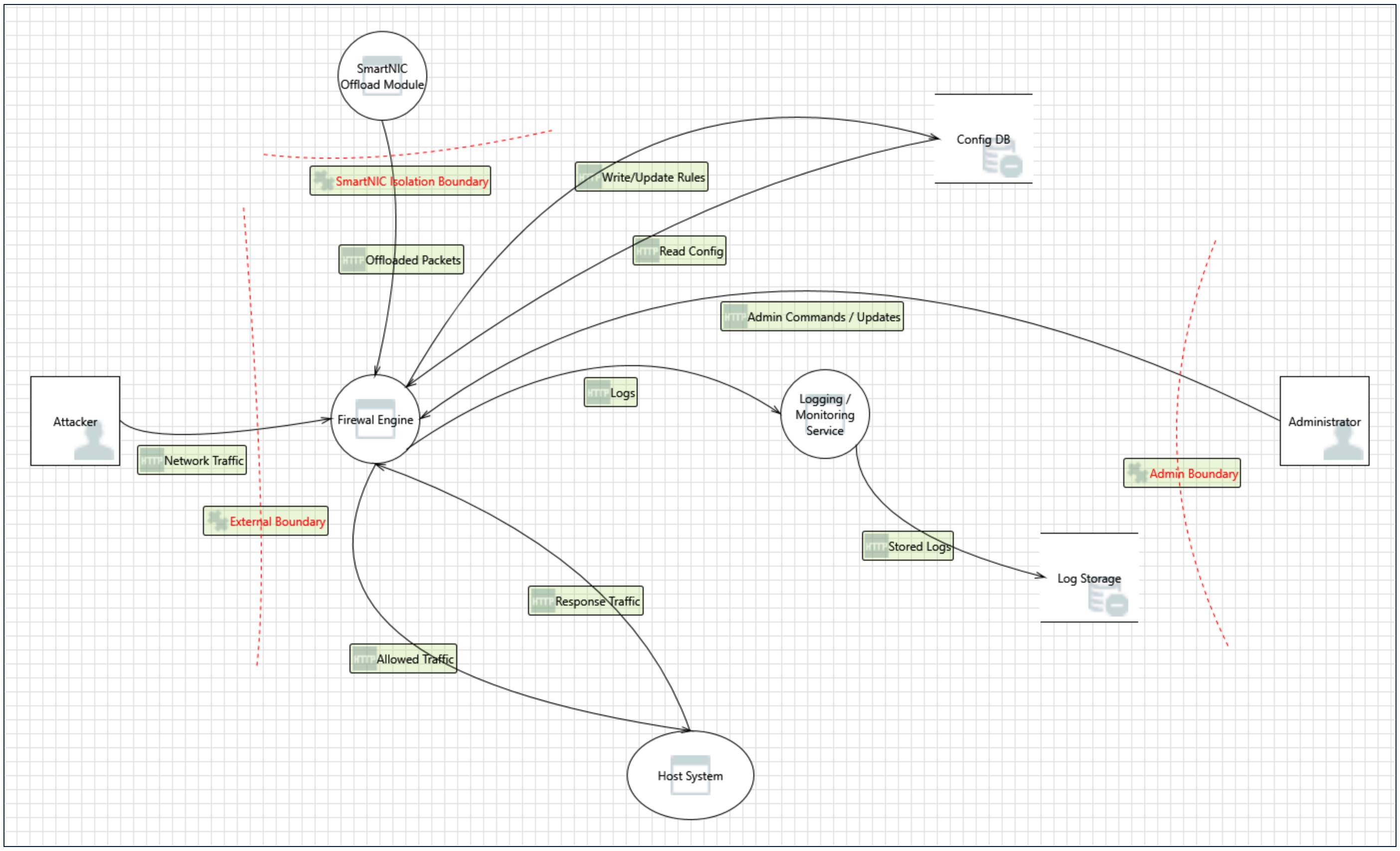
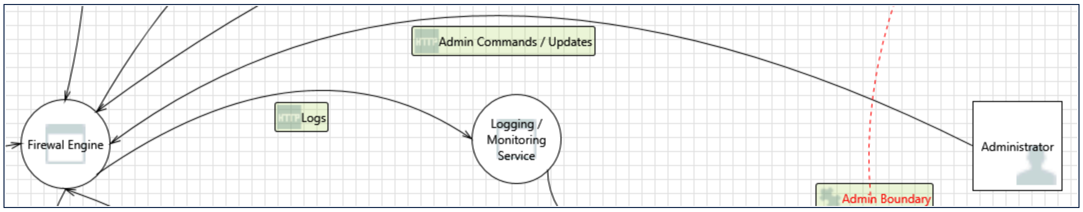


Diagram 1 Diagram Summary:

Not Started	26
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	13
Total	39
Total Migrated	0

Interaction: Admin Commands / Updates



1. Spoofing the Administrator External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Administrator may be spoofed by an attacker and this may lead to unauthorized access to Firewal Engine. Consider using a standard authentication mechanism to identify the external entity.
Justification: Administrative access must be protected so attackers cannot pose as an admin. Strong authentication such as MFA, certificates, or secure keys should be required for any configuration changes. Restrict access to the admin interface and maintain a detailed audit trail so that administrator actions can't be forged. These measures reduce the likelihood of admin-level spoofing, so the threat is mitigated.

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

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

3. Spoofing the Firewal Engine Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Firewal Engine may be spoofed by an attacker and this may lead to information disclosure by Administrator. Consider using a standard authentication mechanism to identify the destination process.
Justification: <no mitigation provided>

4. Potential Lack of Input Validation for Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Admin Commands / Updates may be tampered with by an attacker. This may lead to a denial of service attack against Firewal Engine or an elevation of privilege attack against Firewal Engine or an information disclosure by Firewal Engine. 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: Administrative commands should be treated as untrusted input until verified. The firewall must validate all incoming admin data for correctness and format, ensuring that commands cannot inject malformed values or unexpected control characters. Using authenticated, encrypted channels such as TLS or SSH prevents manipulation in transit, and enforcing strict parameter validation protects the firewall from tampered or malicious updates. With these safeguards in place, the risk of tampering with admin commands is mitigated.

5. Potential Data Repudiation by Firewal Engine [State: Not Started] [Priority: High]

Category: Repudiation
Description: Firewal Engine 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>

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

Category: Information Disclosure
Description: Data flowing across Admin Commands / Updates 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>

7. Potential Process Crash or Stop for Firewal Engine [State: Not Started] [Priority: High]

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

8. Data Flow Admin Commands / Updates 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>

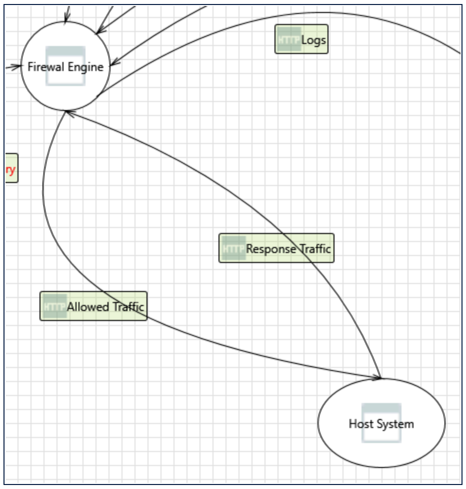
9. Firewal Engine May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Administrator may be able to remotely execute code for Firewal Engine.
Justification: <no mitigation provided>

10. Elevation by Changing the Execution Flow in Firewal Engine [State: Not Started] [Priority: High]

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

Interaction: Allowed Traffic



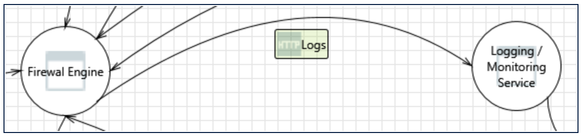
11. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Host System may be able to impersonate the context of Firewal Engine in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: Logs



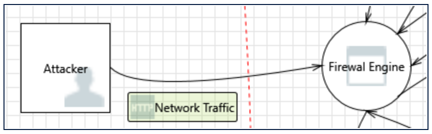
12. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Logging / Monitoring Service may be able to impersonate the context of Firewal Engine in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: Network Traffic



13. Spoofing the Attacker External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Attacker may be spoofed by an attacker and this may lead to unauthorized access to Firewal Engine. Consider using a standard authentication mechanism to identify the external entity.

Justification: To prevent an attacker from pretending to be a trusted external source, the firewall should verify the legitimacy of all incoming traffic. This includes using basic anti-spoofing techniques like ingress filtering, checking source addresses, and validating packet headers. The firewall should only accept traffic from networks we explicitly trust. With these controls in place, this spoofing risk is considered mitigated.

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

Category: Elevation Of Privilege

Description: Firewal Engine may be able to impersonate the context of Attacker in order to gain additional privilege.

Justification: <no mitigation provided>

15. Spoofing the Firewal Engine Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Firewal Engine may be spoofed by an attacker and this may lead to information disclosure by Attacker. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

16. Potential Lack of Input Validation for Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Network Traffic may be tampered with by an attacker. This may lead to a denial of service attack against Firewal Engine or an elevation of privilege attack against Firewal Engine or an information disclosure by Firewal Engine. 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: The firewall should never trust raw network traffic. All packets must be checked to ensure the Ethernet, IPv4, and TCP headers are well-formed and consistent. Malformed or suspicious packets should be dropped before they reach deeper logic. This protects the firewall from corrupted inputs and prevents attacks that rely on packet manipulation. With proper validation in place, this risk is mitigated.

17. Potential Data Repudiation by Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Firewal Engine 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: To prevent disputes about packet origins, the firewall should keep clear and tamper-resistant logs of all traffic entering from the external network. These logs should include timestamps and relevant metadata. Storing logs securely ensures they can't be altered later, which allows us to reliably trace events. With proper logging in place, this threat is mitigated.

18. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Network Traffic 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: Traffic traveling across untrusted network segments should use encryption whenever possible. This prevents attackers from capturing or reading sensitive packet contents. Limiting access to monitoring interfaces and segmenting network paths further reduces exposure. With encryption and access controls applied, this risk is mitigated.

19. Potential Process Crash or Stop for Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Firewal Engine crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The firewall must handle unexpected or malformed packets safely. By performing strict bounds checking and validating every header length before use, we avoid crashes caused by invalid input. Adding watchdog timers and rate limits helps ensure the firewall remains responsive even under heavy load. With proper validation and defensive coding, this DoS risk is mitigated.

20. Data Flow Network Traffic 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>

21. Firewal Engine May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Attacker may be able to remotely execute code for Firewal Engine.

Justification: The firewall engine must be hardened to prevent attackers from injecting or executing their own code. This involves using safe parsing routines, avoiding dangerous memory operations, enabling stack protections, and compiling with security features like ASLR and stack canaries. These protections make remote code execution significantly harder, so the threat is mitigated.

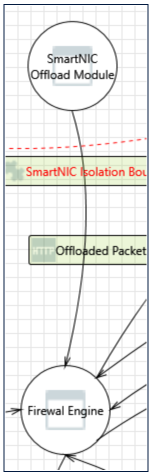
22. Elevation by Changing the Execution Flow in Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Firewal Engine in order to change the flow of program execution within Firewal Engine to the attacker's choosing.

Justification: To stop attackers from manipulating the firewall's execution flow, all external data must be validated before being used by the firewall. Memory safety techniques, strict bounds checking, and compiler hardening help prevent control-flow attacks. Dropping malformed packets prevents attacker-controlled data from influencing execution. With these safeguards, the threat is mitigated.

Interaction: Offloaded Packets



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

Category: Elevation Of Privilege

Description: Firewal Engine may be able to impersonate the context of SmartNIC Offload Module in order to gain additional privilege.

Justification: <no mitigation provided>

24. Spoofing the SmartNIC Offload Module Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: SmartNIC Offload Module may be spoofed by an attacker and this may lead to unauthorized access to Firewal Engine. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

25. Spoofing the Firewal Engine Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Firewal Engine may be spoofed by an attacker and this may lead to information disclosure by SmartNIC Offload Module. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

26. Potential Lack of Input Validation for Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Offloaded Packets may be tampered with by an attacker. This may lead to a denial of service attack against Firewal Engine or an elevation of privilege attack against Firewal Engine or an information disclosure by Firewal Engine. 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: Packets processed by the SmartNIC should also be validated when they return to the firewall. The system should confirm that SmartNIC-generated metadata and classifications are complete and accurate. If anything looks off or inconsistent, the packet should be rejected. Adding this extra validation layer ensures the offload path cannot be abused, so the threat is mitigated.

27. Potential Data Repudiation by Firewal Engine [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Firewal Engine 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: Traffic handled by the SmartNIC should also be logged so that both the SmartNIC and firewall actions can be traced. These logs should record when the offload occurs, how packets were classified, and which component handled them. Keeping these logs in a protected storage area ensures neither device can deny what happened, mitigating the threat.

28. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Offloaded Packets 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: The communication path between the SmartNIC and firewall should be protected so attackers can't observe packet data or inspection results. This may include hardware isolation, secure DMA regions, or encrypting metadata exchanged over the offload channel. These measures prevent eavesdropping on the SmartNIC path, mitigating the threat.

29. Potential Process Crash or Stop for Firewal Engine [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Firewal Engine crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

30. Data Flow Offloaded Packets 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>

31. Firewal Engine May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: SmartNIC Offload Module may be able to remotely execute code for Firewal Engine.

Justification: <no mitigation provided>

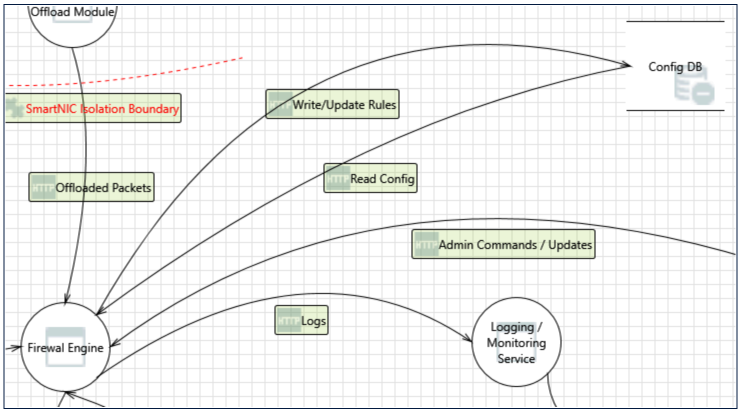
32. Elevation by Changing the Execution Flow in Firewal Engine [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Firewal Engine in order to change the flow of program execution within Firewal Engine to the attacker's choosing.

Justification: <no mitigation provided>

Interaction: Read Config



33. Spoofing of Source Data Store Config DB [State: Not Started] [Priority: High]

Category: Spoofing

Description: Config DB may be spoofed by an attacker and this may lead to incorrect data delivered to Firewal Engine. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

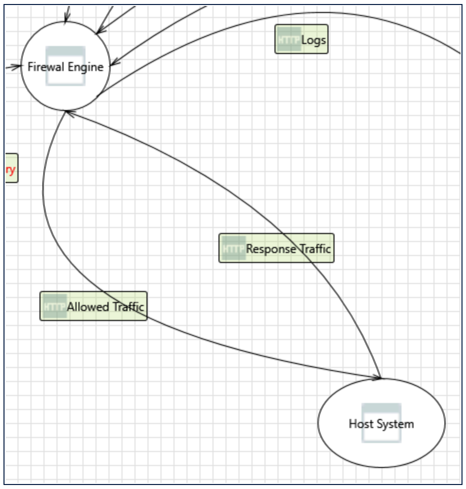
34. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Config DB can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: <no mitigation provided>

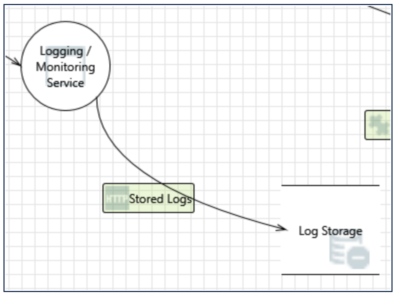
Interaction: Response Traffic



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

Category: Elevation Of Privilege
Description: Firewal Engine may be able to impersonate the context of Host System in order to gain additional privilege.
Justification: <no mitigation provided>

Interaction: Stored Logs



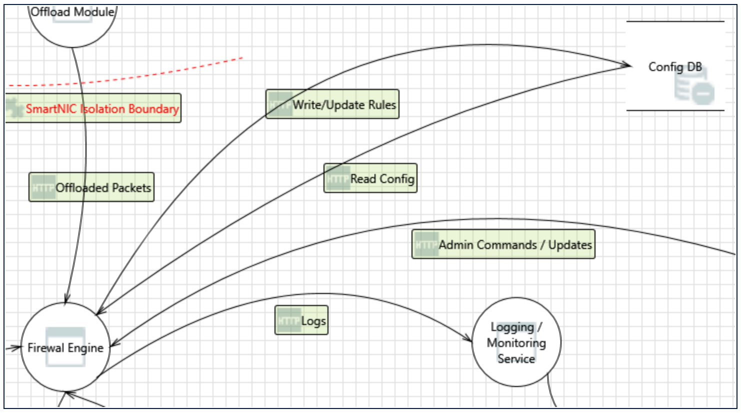
36. Spoofing of Destination Data Store Log Storage [State: Not Started] [Priority: High]

Category: Spoofing
Description: Log Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Log Storage. Consider using a standard authentication mechanism to identify the destination data store.
Justification: <no mitigation provided>

37. Potential Excessive Resource Consumption for Logging / Monitoring Service or Log Storage [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Logging / Monitoring Service or Log Storage 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: Log generation should be controlled so the firewall can't be overwhelmed by excessive logging. This includes limiting log rates, rotating logs regularly, and enforcing size caps. Logging should also be handled asynchronously so it doesn't block packet processing. These controls prevent log-related resource exhaustion, mitigating the threat.

Interaction: Write/Update Rules



38. Spoofing of Destination Data Store Config DB [State: Not Started] [Priority: High]

Category: Spoofing

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

Justification: <no mitigation provided>

39. Potential Excessive Resource Consumption for Firewal Engine or Config DB [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does Firewal Engine or Config DB 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>