|  |
| --- |
| Zorg Industries |
|  |

# Memorandum

To: Hari Seldon CEO

From: Chad Ballay

Subject: Firewall Project Review and Recommendations

# Project Status

|  |  |  |
| --- | --- | --- |
| **Epic** | **Status** | **Callout** |
| Endpoint | Green | Desktop Support has been a key partner. |
| Cloud/Compute | Green | Build process phase nearing completion. |
| Segmentation | Yellow | Continued discovery of Shadow IT infrastructure. |
| DMZ | Red | Legacy application modifications have blocked progress. |

# Background

Recent data breaches and penetration tests have confirmed that our current security posture has several deficiencies. As part of the broader initiative we are establishing an enterprise initiative to strengthen our current firewall offerings. We are aligning the epics within this initiative along firewall technologies to allow for specialist teams to move at their own independent pace rather than aligning to business segments. Most epics will require a mix of the three basic firewall subtypes. (Guidelines on Firewalls and Firewall Policy, n.d.)

**Packet Filtering**—Firewall implementation that inspects individual packets and applies rules on a case by case basis.

Stateful Inspection – Firewall implementation that is session aware and to implement context for filtering.

Application Proxy – Next generation firewall that evaluates traffic in an application specific context for filtering.

# Current Update

**Endpoint Firewalls - GREEN**

Desktop firewalls are being rolled out through our Symantec Endpoint manager. For each business area we’ll use the rollout policy of targeted communication, initial install with no rules enabled, phase 1 rules installed, phase 2 rules installed, support handoff to Desktop Support. Impact has been minimal. (Host-based Firewall Software Guidelines, n.d.)

**Cloud Firewalls - GREEN**

Build guidelines and policies have been developed. Automation is underway to ensure compliance. Monitoring tooling and implementation not begun yet. Test and QA piloting begun. (What is Azure Firewall?, n.d.) (Quickstart: Deploy Azure Firewall with Availability Zones - Resource Manager template, n.d.)

**Segmentation Firewalls – YELLOW**

We have discovered additional orphaned IT infrastructure that has been maintained by the business and is out of compliance with current policies across multiple fronts. We have been performing minor GAP analyses to triage project impact but many of these have significant deficiencies before we can begin our own efforts. Epic timelines are in jeopardy if we include this in our scope. (Chandramouli, n.d.)

**DMZ Firewalls – RED**

Core business services currently rely on several legacy applications that are vendor sourced and are unable to be modified sufficiently. Implementation of needed modifications is being reviewed between our subject matter experts, vendor management office, and vendor client managers to see what falls under our existing Master Services Agreement and what will require an additional Statement of Work. Epic is at risk due to contractual agreements and budget. (Enterprise Internet Edge, n.d.) (Secure Architecture Design Definitions, n.d.)

# Bibliography

**Much of the references here are for background context of goals and not reference of actual designs.**

Chandramouli, R. (n.d.). *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*. Retrieved from NIST Special Publication: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf

Clayton, R. (n.d.). *Fortnite’s Vulnerability: Only the Secure Survive*. Retrieved from Check Point Blog: https://blog.checkpoint.com/wp-content/uploads/2019/01/Fortniteblog1.png

*Enterprise Internet Edge*. (n.d.). Retrieved from Cisco SAFE Reference Guide: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE\_RG/SAFE\_rg/chap6.html

*Guidelines on Firewalls and Firewall Policy*. (n.d.). Retrieved from COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

*Host-based Firewall Software Guidelines*. (n.d.). Retrieved from Berkley Information Security Office: https://security.berkeley.edu/MSSND/host-based-firewall-software-guidelines

*Quickstart: Deploy Azure Firewall with Availability Zones - Resource Manager template*. (n.d.). Retrieved from Microsoft Azure Documentation: https://docs.microsoft.com/en-us/azure/firewall/deploy-template

*Secure Architecture Design Definitions*. (n.d.). Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.us-cert.gov/ics/Secure-Architecture-Design

*What is Azure Firewall?* (n.d.). Retrieved from Microsoft Azure Documentation: https://docs.microsoft.com/en-us/azure/firewall/overview