You are working with your manager on a project. You are attempting to determine the best approach for securing inbound traffic from the Internet to various application servers on the client’s local area network (LAN). You would like to select a strategy that gives the client significant control over user accessibility. You would also like to ensure that all data passing into your client’s network is properly evaluated before access is granted. Integrity of data is the top priority; however, your client has a limited budget for deployment.

Using the information presented above, discuss which of the following firewall security strategies would be a good fit for your client’s network environment.

**Firewall Security Strategies**

**Security through obscurity**

By configuring systems in a way that does not follow normal patterns and is not easily understandable, security through obscurity can be obtained. By utilizing abnormal configurations, the probability of exploitation is reduced and a level of protection is obtained. Administrators seek security through obscurity by performing one or more of the following actions:

* Modification of default ports
* Spoofing of banners or headers
* Utilization of extraordinary long Uniform Resource Locators (URLs)
* Utilizing uncommon protocols or operating systems

Keep in mind that this strategy may instill a false sense of security. Because attackers have multiple methods to scan against system configurations, utilizing this as the only security mechanism is like using nothing at all.

**Least privilege**

This strategy requires that each user or group that requires access to resources be explicitly granted permission. Because all resource access would be denied by default, each individual access need would have to be individually addressed. When least privilege is employed, there is often a dramatic increase in administrative overhead as a direct result. Least privilege is preferred for administrative scenarios.

**Simplicity**

This strategy reinforces that the selected solution should remain simple. By retaining a simple solution, the potential for error in configuration, bugs, or other problems is reduced.

**Defense in Depth**

This strategy emphasizes on a layered approach. The use of multiple safeguards ensures that no system that represents a single point of failure could be breached. The characteristics of a defense-in-depth strategy are:

* Public networks are separate from private networks
* Multiple security controls are implemented
* Redundant security controls are implemented
* Consists of multiple tiers or layers

**Diversity of Defense**

Diversity of defense is similar to defense in depth in terms of layered approach. The distinction is that diversity in defense represents each of those layers with a different technology.

**Chokepoint**

A chokepoint forces all traffic through a single pathway to ensure that security checks take place. This strategy is only valuable if the chokepoint is hard to bypass or skip around. Additionally, because all traffic is funneled into the single pathway, issues regarding bandwidth constraints or performance problems may arise.

**Weakest Link**

Because all environments have a weakest link, this strategy subscribes to the continuous process of identifying the weakest link and eradicating it.

**Fail-safe**

Failure is destined to occur on security systems, and when it does a strategy for handling the failure should already be in place. When a failure occurs and a fail-safe is triggered, there are two possible reactive choices:

* Fail-open: Security systems fail, but in order to maintain availability network communications are allowed to continue.
* Fail-closed: When security fails in order to retain security and integrity, the network pathway is closed and traffic flow does not continue.

Fail-safe is a strategy that is most often used in conjunction with other strategies.

**Forced Universal Participation**

When it comes to selecting a security strategy it is important that all users and groups involved in its execution are supportive. End users are a potentially exploitable key for an attacker to utilize in order to gain unauthorized access to a network environment. When end users intentionally or inadvertently do not follow security principals, an attacker can more readily cause a breach in the security systems. A good example of this is when users write down their user name and password information and store them in plain sight. Without buy-in to the selected security strategy and a commitment to following protocol, there is a higher probability for breach. Selecting and following through with the implementation of a forced universal participation strategy will ensure that security policies are observed.