

Where is Application Protection Best Applied?

Shawn Nunley, NetScaler

... at a proxy, in front of application

⇒ PROS

- Protocol-level attacks stopped before they can compromise app server
- Proxies can aggregate traffic of many servers and apply a consistent security policy
- Application servers need only be optimized for the application (not security measures)
- To application, all clients are well-connected network clients (not slow, lossy)

... at a proxy, in front of application

⇒ More Pros...

- Enables centralized logging (if proxy can see server responses)
- Heavy-duty work can be off loaded from application server (e.g. pre-processing of XML or SSL termination)
- Reduces the need for "fire drill" patching for new vulnerabilities across server farms

Cons

- ⇒ Can impact logging (could be a positive effect)
- ⇒ Yet another device to manage
- ⇒ Possible latency hit
- ⇒ Applications aren't designed with a proxy in mind. Some applications are not well behaved.

... **what makes a good proxy?**

- ⇒ Ability to process encrypted traffic
- ⇒ Performance impact
(positive, neutral or negative?)
- ⇒ *Real* Transparency - some applications may require direct connection to client
- ⇒ Manageability
- ⇒ Depth and breadth of security policy control
(deep packet inspection, virus scanning, etc)