Checklist for Secure Application Delivery

Inbound from User

1	Proxy the TCP session (and protect against DoS attacks)
2	Decrypt the SSL stream
3	Normalize the user session into a canonical character set
4	Translate URL addresses from exterior to interior DNS namespaces
5	Re-write HTTP headers
6	Inspect for proper credentials and redirect to an AAA system if necessary
7	Check against URL access lists
8	Check embedded HTTP parameters against parameter ACLs
9	Inspect for cookie tampering
10	Inspect for forms tampering
11	Evaluate all fields for buffer overflows
12	Check for application attacks such as SQL injection and JavaScript injection
13	Verify max-length and other requirements stated by the application
14	Check cache for serving static content
15	Queue up traffic if the application is nearing capacity limits
16	Load balance traffic
17	Securely log each transaction and security exception
18	Connect to the server using an open pooled TCP connection

Outbound to User

19	Translate URLs back to exterior DNS namespace
20	Re-write session content
21	Encrypt cookies and/or digitally sign them
22	Gather field, link, and parameter data to validate against future inputs
23	Cloak all identifying banners and content, and normalize error codes
24	Mask credit card numbers, Social Security numbers, and other sensitive data
25	Optimize for WAN delivery using compression or TCP optimizations
26	Encrypt
27	Send to the user

Delivery Security Both