NetScaler Web Application Firewall Jump Start

NetScaler Web Application Firewall is a security solution that protects web applications and APIs from a wide range of cyber threats. Unlike traditional network firewalls that inspect traffic at the network level (Layers 3 and 4), a WAF operates at the application layer (Layer 7), enabling it to understand and analyze web protocols like HTTP, XML, and JSON.

NetScaler Web Application Firewall (WAF) Jump Start is designed to provide customers with the base knowledge and experience for deploying and managing WAF for protecting NetScaler hosted applications.
NetScaler WAF filters requests and responses for malicious activity. It uses a one-pass architecture to process traffic, which reduces latency and improves application performance.

Some of the key features and benefits of NetScaler WAF:

- Hybrid Security Module: NetScaler WAF employs a hybrid security model, combining both positive and negative security approaches.
- IP Reputation blocking black-listed IP addresses dynamically updated every 5 minutes from the Webroot database
- Protect against known and unknown attacks including OWASP top 10 and zero-day threats
- Uses a one pass architecture for traffic process which provides the most efficient L4-L7 inspection without compromising application performance.
- Specialized Internet Bot protection

NetScaler Web Application Firewall Jump Start will include the following high-level objectives:

The NetScaler Console Services is leveraged for discovery and to provide analytics. The NetScaler Console Service will be provisioned as an optional phase if it does not exist. The ADM Agent is required for configuration packs and analytics, if an agent does not exist, one will be deployed and added to the Console Service. The NetScaler WAF Firewall Jumpstart will be limited to one vServer and extend over approximately one week to obtain sufficient visibility and testing with the protected application. The customer has the option of using a parallel test vServer hosted on the same NetScaler or another instance running the same firmware version to test the WAF protections and generate learned data. The WAF profile will be finalized and implemented during an approved change window.

The NetScaler WAF deployment includes the following objectives:

- NetScaler WAF Configuration
- IP Reputation
- Bot protection
- Discovery and WAF recommendations
- Deployment of profiles, policies and signatures
- Enable NetScaler Console security analytics

At the conclusion of the engagement and after enabling the WAF profile, Choice Solutions and the customer will meet for a review and open question and answer to ensure the customer can successfully move forward using the NetScaler WAF and NetScaler Console Security analytics.