Benötigte Daten bei der Erstkonfiguration der Honeywall.

Abschnitt 1
Grundkonfiguration für die Honeypots.

IP Adresse des Honeypots (Beispiel: 10.0.0.20)
Netzwerkgrösse (Beispiel: 10.0.0.0/24)
Broadcast Adresse (Beispiel: 10.0.0.255)

Abschnitt 2
Management Interface

Netzwerkkarte (Beispiel: eth2)
IP Adresse (Beispiel: 10.10.10.66)
Subnetmaske (Beispiel: 255.255.255.0)
Default Gateway (Beispiel: 10.10.10.1)
Hostname (Beispiel: honeywall)
DNS Domain (Beispiel: honeywall.firma.com oder localhost)
DNS Server IP
Interface aktivieren (Ja / Nein)
Interface beim booten aktivieren (Ja / Nein)
SSH konfigurieren (Ja / Nein)
SSH Port (Default: 22)
Root erlauben sich direkt über SSH einzuloggen (Ja / Nein)
Root Passwort ändern (Ja / Nein)
Das neue Passwort für Root
SSHD beim booten automatisch starten (Ja / Nein)
SSH Einstellungen speichern und Dienst neu starten (Ja / Nein)

Über welche Ports darf auf das Interface zugegriffen werden? (Default: 22 443)
IP Adresse die auf das Interface zugreifen darf.
Web Interface für Analyse und Management aktivieren? (Ja / Nein)
Firewall Begrenzung von innen nach aussen aktivieren? (Ja / Nein)
TCP Ports nach aussen offen (Default: 22 25 43 80 443)
UDP Ports welche nach aussen offen sind (53 123)

Abschnitt 3
Firewalleinstellungen

Periode der Verbindungslimite (englische Angabe, Default: hour)
TCP Limite pro Periode (Default: 20)
UDP Periode pro Periode (Default: 20)
ICMP Limite pro Periode (Default: 50)
Andere Verbindungsarten pro Periode (Default: 10)
Firewall sendet Pakete an Snort_Inline (Ja / Nein)
Einstellung von Snort_Inline
Blacklist
Whitelist
Black- und Whitelist filtern
Fencelist
Fencelist filtern
Disallow any traffic outbound from honeynet
Unlimitierte DNS Zugriffe
Honeypots festlegen welche über unlimitierte DNS Zugriffe verfügen
IP Adresse der Honeypots

DNS Server IP
eMail Alarmierung aktivieren
eMailadresse
eMail Alarmierung beim booten aktivieren?
Sebek Variablen konfigurieren
Ziel IP der Sebek Pakete
UDP Port der Sebek Pakete
Sebek Paket Optionen