# Implementation Service Description (ISD)
# Juniper Firewall SSG

**ISD Bezeichnung: Juniper_Firewall_SSG_V01_DE**
**Ausgabe: Februar 2011**

## 1.0 Grundlagen der Implementierung

Diese ISD ist eine Anlage zum Vertrag zwischen Avaya GmbH & Co. KG (nachfolgend „Avaya“) und dem Kunden. Zusätzlich finden die „Bedingungen für Implementierungsleistungen“ in der jeweils aktuellen Fassung Anwendung.

## 2.0 Produktspezifische Leistungen

### 2.1 Die Einrichtung der Firewall durch Avaya beinhaltet:

- Inspizieren der Lieferung auf vollständige Hardware und Lizenzen.
- Prüfen der bauseits vorhandenen Netzwerkanschlüsse für die zu installierende Firewall.
- Einmalig Aktualisierung der Firmware auf aktuelle empfohlene Version des Herstellers zum Zeitpunkt der Installation.
- Installation und Konfiguration der Firewall und folgender Parameter:
  - Drei Zonen: Trust, Untrust und DMZ (DeMilitarisedZone)
  - Basiskonfiguration (Name, Standort und Kontakt, DNS-Server, Datum, Zeitzone und Sommerzeit)
  - Systemzeit über einen Internet-Zeitserver per SNTP (Simple Network Time Protocol)
  - NAT (Network Adress Translation) und „Alles-erlaubt“ Firewallregel von Trust und DMZ nach Untrust
  - Administrator mit Leserechte und Administrator mit Schreib- und Leserechte
  - IP-Adresse und Netzwerkmaske je Zone
  - Standard Gateway
- Verbindung der Firewall an die Stromversorgung und an die am Einbauort befindlichen Netzwerkgeräte (z. B. Router des Leitungsanbieters, Kundenswitch).
- Wenn beim Kunden vorhanden: Einbau der Firewall in 19-Zoll-Schrank.
- Wenn vom Kunden bestellt: Einspielen der Extended-Lizenz für SSG5.
- Wenn vom Kunden bestellt: Konfiguration NSRP Hochverfügbarkeit an einer zweiten Firewall.
- Inbetriebnahme der Firewall.
- Soweit vom Kunden ein Wartungsservice mit einer Serviceklasse beauftragt wurde, die Remote-Zugang beinhaltet: Anbindung an das Remote Management System und Registrierung der Firewall beim Hersteller.
- Kurztest der Firewalls.
- Sicherung und Archivierung der Konfiguration zum Zeitpunkt der Übergabe des Systems.
- Dokumentation der Konfigurations- und Zugangs- daten und Bereitstellung für den Kunden in elektronischer Form per E-Mail mit einem PDF-Anhang.
- Einmalige, maximal 15-minütige Kurzeinweisung wie man auf die Weboberfläche und die SSH Shell kommt.

### 2.2 Zusätzliche Leistungen

Zusätzliche Leistungen, die

- über die Standardimplementierung hinausgehen, oder
- optionale Leistungen gemäß Ziffer 4.0 darstellen, oder
- durch die nicht zeitgerechte oder nicht vollständige Bereitstellung der unter Ziffer 3.0 genannten Mitwirkungs- und Beistellungsleistungen verursacht werden,

werden von Avaya jeweils nach tatsächlichem Aufwand zu den dann jeweils gültigen Listenpreisen berechnet.

## 3.0 Mitwirkungspflichten und Beistellungen des Kunden

- Der Kunde stellt die für die Konfiguration erforderlichen Daten zur Verfügung (Name, Standort, eine IP-Adresse für einen Servicetechniker und eine je Zone [bei Hochverfügbarkeit drei], Standard Gateway und DNS-Server).
- Der Kunde stellt alle Kontaktdaten incl. Geschäftszeiten der Ansprechpartner zur Verfügung die Avaya zur Installation und Installationsvorbereitung benötigt. Zu den Kontaktdaten gehört sofern vorhanden Telefonnummer Festnetz und Mobil sowie eine Email-Adresse. ggf. auch ein Eskalationspfad.
- Routingtabellen und Netzwerkkonfiguration einzelner Geräte auf Anfrage.

### 3.1 Netzwerk Voraussetzungen

Mindestvoraussetzungen:

- Fehlerfreie Cat5e oder höher Verkabelung.
- Fehlerfreies Switching und Routing innerhalb der Kundennetze.

### 3.2 Power Management Voraussetzungen

Nicht zutreffend

### 3.3 Lizenz Voraussetzungen

Nicht zutreffend

### 3.4 Hardware Voraussetzungen

- Der Kunde stellt einen Netzwerkanschluss je genutzter Schnittstelle für die Firewall zur Verfügung. Die vom Kunden zur Verfügung gestellten Netzwerkschnittstellen müssen auf „Automatische Aushandlung von Duplex und Geschwindigkeit“ stehen. Feste Einstellungen sind gegenüber dem Vor-Ort Techniker zu benennen.
- Der Kunde stellt ein Ethernet-Kabel der Kategorie 5e oder höher mit RJ-45-Anschlüssen für jede Schnittstelle der Firewall die er anschließen will. Jedes Ethernet-Kabel darf höchstens 100 m lang sein.
- Der Kunde trägt dafür Sorge, dass sich alle Netzwerkanschlüsse für die Firewall, insbesondere der Internetanschluss, in Reichweite der Firewall befinden, so dass diese mit den vom Kunden zur Verfügung gestellten Ethernet-Kabeln erreicht werden können.
- Bei DSL-Anschlüssen ohne Providerrouter, in der Regel T-DSL Business oder T-DSL Home, stellt der Kunde ein DSL-Modem z.B. Telekom Speedport 201. Ein DSL-Router ist NICHT geeignet. Ausfälle und Störungen des DSL-Modems sind durch keinen Avaya-Servicevertrag abgedeckt.

- Bereitstellung des Stromanschlusses für die Firewall. Dieser muss sich im gleichen Raum in Reichweite des Aufstellungsorts der Firewall befinden.
- Bereitstellung von ausreichend Aufstellungsplatz (im Maße der Abmessung des Gerätes) zum Einbau der Firewall in einen 19-Zoll-Schrank oder zum Aufstellen an einem von äußeren Einflüssen, wie Wasser, Schmutz, Frost und Hitze, geschützten Ort.
- Für den Einbau eines nicht-19-Zoll Gerätes, wie der SSG5 in einen 19-Zoll-Schrank, ist ein Fachboden zur Verfügung zu stellen oder ein Einbaurahmen mitzubestellen. Auf einem Fachboden darf das Gerät nur neben und nicht auf oder unter einem anderen Gerät stehen. Ist dies nicht möglich weil der Fachboden schon ausgelastet ist, ist ein eigener Fachboden für die SSG5 zur Verfügung zu stellen.
- Für den Einbau in einen 19-Zoll-Schrank stellt der Kunde pro Firewall vier Käfigmuttern und vier zugehörige Schrauben zur Verfügung.
- Der Kunde trägt dafür Sorge, dass die Temperatur innerhalb des 19-Zoll-Schrankes die für die Firewall zulässigen Temperaturen während des ganzen Jahres nicht überschritten werden. Dies bedeutet ggf. den Einbau von Lüftern, Klimaanlagen und Heizungen.
- Wandmontage sofern möglich obliegt dem Kunden.
- Bei Hochverfügbarkeit ohne Schnittstellenvirtualisierung stellt der Kunde einen konfigurierbaren, VLAN-fähigen Ethernet-Switch. Jede Schnittstelle, die an der Firewall hochverfügbar sein soll, muss auf dem Switch als eigenes VLAN eingerichtet werden. Das jeweilige VLAN enthält eine Schnittstelle für die Hauptfirewall, eine für die Sicherungsfirewall und die benötigte Anzahl an Schnittstellen für die anzuschließenden Netzwerkgeräte. Zusätzlich wird eine Ethernet-Verbindung zwischen den Firewalls benötigt. Diese Verbindung kann auch über ein separates VLAN durch ein Netzwerk geführt werden.

### 3.5 Software Voraussetzungen

Zugang zur Firewall:

- Internetbrowser: Microsoft Internet Explorer 7.0 oder neuer, Firefox 3.6 oder neuer
- SecureShell: Putty 0.60 oder neuer

### 3.6 Produktspezifische Sicherheitsmaßnahmen

Nicht zutreffend

## 4.0 OPTIONALE LEISTUNGEN

Nachfolgende Leistungen sind nur dann Bestandteil dieser Implementation Service Description (ISD) wenn sie vom Kunden jeweils gesondert schriftlich beauftragt wurden.

### 4.1 Anwenderberatung je 15 Min. innerhalb der Geschäftszeit, #219.169.582

#### 4.1.1 Produktspezifische Leistungen

- Produktspezifische Beratung und Beratung in dessen Umfeld.

#### 4.1.2 Voraussetzungen

Alle notwendige Informationen auf deren Grundlage das Gespräch stattfinden soll.

### 4.2 Systemspezialist je Stunde innerhalb der Geschäftszeit, #219.169.728

#### 4.2.1 Produktspezifische Leistungen

- Kundenindividuelle Implementierung nach Aufwand (z. B. Unterstützung bei Einrichtung der VLANs bei Hochverfügbarkeit, Ende-zu-Ende VPN, Mobiles VPN, Benutzerprofilerstellung für Mobiles VPN, kundenspezifisches Firewall-Regelwerk incl. Aliaskonfiguration, Unterstützung bei Portermittlungen für Kundenprogramme, Dynamisches Routing über OSPF (Open Shortest Path First), Rückfallmechanismen über Schnittstellenüberwachung, Lastverteilungsmechanismen, Multi-Internet Anbindung, Schnittstellenvirtualisierung auch im Zusammenhang einer Hochverfügbarkeit, Webfilterimplementation).

#### 4.2.2 Voraussetzungen

Alle notwendigen Informationen um die jeweiligen Leistungsmerkmale zu implementieren. Dies sind z.B.

- Für ein kundenspezifisches Firewall-Regelwerk liefert der Kunde das Regelwerk selbst, alle IP-Adressen, zugehörige Namen und deren jeweilige Gruppenzugehörigkeit. Ebenso die genutzten Protokolle und sofern diese kein Standard sind auch die genutzten TCP bzw. UDP Ports.
- Benutzernamen, Passwörter und Email-Adressen bei Mobile User VPN, VPN-Parameter für Site-to-Site VPN, Kontaktdaten des Ansprechpartners der VPN-Gegenstelle.
- Der Kunde stellt sicher, dass bei einer Site-to-Site VPN Einrichtung der Ansprechpartner der Gegenstelle zum Einrichtungszeitpunkt bis zur einwandfreien Herstellung des VPNs zur Verfügung steht.
- Rückroute im Standard Gateway zum jeweiligen neuen VPN-Netz sofern die Firewall nicht Standard Gateway ist.
- Sollen Ports ermittelt werden muss der Kunde in der Lage sein den Dienst auf Anfrage zu starten.
- Für VPN-Verbindungen stellt der Kunde eine öffentliche IPv4 IP-Adresse an dem jeweiligen Internetanschluss pro Firewall bzw. pro Hochverfügbarkeitsverbund.
- Webfilter-Subskriptionscodes müssen für die Webfilterimplementation gestellt werden. Der Kunde ist für die Gültigkeitsdauer der Subskription verantwortlich und stellt rechtzeitig einen neuen Code zum Einspielen zur Verfügung. Das Einspielen des neuen Codes ist kostenpflichtig.