

Implementation Service Description (ISD) - Defendo Appliance

ISD Bezeichnung: Defendo_V01_DE
Ausgabe: September 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 Defendo Appliance durch Avaya beinhaltet:

- Überprüfen der Lieferung auf vollständige Hardware und Lizenzen.
- Prüfen der kundenseitig vorhandenen Netzwerkanschlüsse für die zu installierende Appliance.
- Einmalig Aktualisierung der Firmware auf aktuelle empfohlene Version des Herstellers zum Zeitpunkt der Installation.
- Konfiguration folgender Funktionen und Parameter der Appliance:
 - Aufteilung des Traffic in zwei Sicherheitszonen: vertraut (Trust) und unvertraut (Untrust).
 - Basiskonfiguration (Name, Standort und Kontakt, DNS-Server, Datum, Zeitzone und Sommerzeit).
 - Systemzeit über einen Internet-Zeitserver per SNTP (Simple Network Time Protocol).
 - NAT (Network Address Translation)
 - Erstellung einer Firewallregel für den Datenverkehr von der Zone vertraut zu der Zone unvertraut, die den gesamten Datenverkehr erlaubt.
 - Administrator mit Vollzugriff für Avaya, Kundenadministrator mit Rechten in Abhängigkeit vom Servicevertrag.
 - IP-Adresse und Netzwerkmaske je Zone.
 - Standard Gateway
 - Einrichtung als Webproxy mit Anti-Virus Funktion entsprechend der vom Kunden bestellten Benutzer und Anti-Virus Lizenzen.
 - Einrichtung des Systems als Email-Relay oder Email-Server mit Anti-Spam und Anti-Virus Funktion entsprechend der vom Kunden bestellten Benutzer und Anti-Virus Lizenzen. Die Einrichtung von Relay-Domänen als auch POP3 und Benutzerkonten ist auf fünf begrenzt. Übernahme einer vorhandenen Konfiguration sofern es sich um ein Hardware-Upgrade handelt.
- Verbindung der Appliance an die Stromversorgung und an die am Einbauort befindlichen Netzwerkgeräte (z. B. Router des Leitungsanbieters, Kundenswitch).
- Wenn beim Kunden vorhanden: Einbau der Appliance in 19-Zoll-Schrank.
- Inbetriebnahme des Systems.
- Soweit vom Kunden ein Wartungsservice mit einer Serviceklasse beauftragt wurde, die Remote-Zugang beinhaltet: Anbindung an das Remote Management System.
- Kurztest der HTTP-Proxy und E-Mailfunktionalität in Zusammenarbeit mit dem Kunden.
- Sicherung und Archivierung der Konfiguration zum Zeitpunkt der Übergabe des Systems.
- Dokumentation der Konfigurations- und Zugangsdaten und Bereitstellung für den Kunden in elektronischer Form per E-Mail mit einem PDF.
- Einmalige, maximal 15-minütige Kurzeinweisung wie man die Weboberfläche erreicht.
- Wenn vom Kunden bestellt: Bei Mobile-User VPN erhält der Kunde zusätzlich per E-Mail eine

Anleitung mit Bildschirmfotos im PDF-Format, die die Einrichtung des Windows-eigenen Clients zeigt. Die Einrichtung am Client wird durch den Kunden durchgeführt.

2.2 Zusätzliche Leistungen

- Zusätzliche Leistungen, die
- über die Standardimplementierung hinausgehen, oder
 - optionale Leistungen gemäß Ziffer 4 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, Standard Gateway, DNS-Server, Domäneninformationen und E-Mail-Server Adressen und ggf. POP3 Zugangsdaten je nach Kundenkonfiguration der E-Mailzustellung).
- Der Kunde stellt alle Kontaktdaten incl. Geschäftszeiten der Ansprechpartner zur Verfügung die Avaya zur Installation und Installationsvorbereitung benötigt. Zu den Kontaktdaten gehören, sofern vorhanden: Telefonnummer Festnetz und Mobil sowie eine E-Mail-Adresse. ggf. auch ein Eskalationspfad.
- Routingtabellen und Netzwerkkonfiguration einzelner Geräte auf Anfrage.
- Änderungen von DNS Einträgen von Kundendomänen sind vom Kunden rechtzeitig zu beantragen und mit Avaya zu abzustimmen.
- **Bei der Defendo sind dies insbesondere:**
 - Die Eintragung der Appliance als Proxy in den Clientsystemen durch den Kundenadministrator oder es muss eine Beauftragung bei Avaya erfolgen.
 - Weitere Domänen, Benutzer und Konten müssen vom Kunden-Administrator eingetragen werden oder es muss eine Beauftragung bei Avaya erfolgen.

3.1 Netzwerk Voraussetzungen

Nicht zutreffend

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 Appliance 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 Appliance, die er anschließen will. Jedes Ethernet-Kabel darf höchstens 100 m lang sein.

- Der Kunde trägt dafür Sorge, dass sich alle Netzwerkanschlüsse für die Appliance insbesondere der Internetanschluss in Reichweite der Appliance befinden, so dass diese mit den vom Kunden zur Verfügung gestellten Ethernetkabeln 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 Appliance. Dieser muss sich im gleichen Raum in Reichweite des Aufstellungsorts der Appliance befinden.
- Bereitstellung von ausreichend Aufstellungsplatz (im Maße der Abmessung des Gerätes) zum Einbau der Appliance 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 in einen 19-Zoll-Schrank ist ein Fachboden zur Verfügung zu stellen. 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 Appliance zur Verfügung zu stellen.
- Für den Einbau in einen 19-Zoll-Schrank stellt der Kunde pro Appliance vier Käfigmuttern und vier zugehörige Schrauben zur Verfügung.
- Der Kunde trägt dafür Sorge, dass die Temperatur innerhalb des 19-Zoll-Schranks die für die Appliance zulässigen Temperaturen während des ganzen Jahres nicht überschritten wird. Dies bedeutet ggf. den Einbau von Lüftern, Klimaanlage und Heizungen.
- Bei Hochverfügbarkeit stellt der Kunde einen konfigurierbaren, VLAN-fähigen Ethernet-Switch. Jede Schnittstelle, die an der Appliance hochverfügbar sein soll, muss auf dem Switch als eigenes VLAN eingerichtet werden. Das jeweilige VLAN enthält eine Schnittstelle für die Hauptappliance, eine für die Sicherheitsappliance und die benötigte Anzahl an Schnittstellen für die anzuschließenden Netzwerkgeräte.

3.5 Software Voraussetzungen

Zugang zur Appliance:

- Internetbrowser: Microsoft Internet Explorer 7.0 oder neuer, Firefox 5 oder neuer
- Mobile User VPN: Windows XP, Vista., 7 mit aktuellen Servicepack und Patches

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 über die Konfigurationsmöglichkeiten und Einsatzmöglichkeit im Kundennetzwerk.

4.1.2. Voraussetzungen

Nicht zutreffend

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. Alias-konfiguration, Portermittlungen für Kundenprogramme, Webmail, Webfilter, erweitertes Spamfiltering z.B. Greylisting, Content-Filtering z.B. Video und Audio-Streams, Dateifilterung, DSCP Priorisierung, Policy Based Routing, Intrusion Detection/Prevention, Active Directory Anbindung, SSL Splitting, Reverse Proxy für MS Exchange).
- Einspielen von Lizenzschlüsseln für zeitbegrenzte Funktionen.
- Konfiguration einer zweiten Defendo Appliance als hochverfügbares System mit der ersten Defendo Appliance.
- Die Eintragung der Appliance als Proxy in den Clientsystemen.
- Weitere Domänen, Benutzer und Konten.

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 E-Mail-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 Appliance 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.
- Für die Anbindung an Active Directory muss ein entsprechendes Zugriffskonto benannt werden. Bei Fragen unsererseits muss ein kompetenter Ansprechpartner erreichbar sein, der die Kundenstruktur des Active Directory kennt.
- Einige Features wie spezielle Varianten des Webfiltering und IDP benötigen zusätzliche Lizenzen.