

Teil der
VSE

VSE **NET**

Öffentlich

Leistungsbeschreibung

Managed Firewall

Das Schutzschild für Ihr Netzwerk



| | |
|---|-----------|
| 1. Allgemeine Informationen | 3 |
| 2. Technische Eigenschaften | 3 |
| 2.1. Hardware | 3 |
| 2.2. Leistungsmerkmale | 3 |
| 2.3. VPN-Zugänge | 6 |
| 2.4. FortiManager | 6 |
| 2.5. FortiAnalyzer | 6 |
| 3. Konfiguration, Installation und Abnahme | 7 |
| 3.1. Konfigurationsworkshop | 7 |
| 3.2. Konfigurationsdokumentation | 7 |
| 3.3. Initiale Konfiguration | 7 |
| 3.4. Installation | 7 |
| 3.5. Abnahme | 7 |
| 3.6. Einweisung | 8 |
| 3.7. Entstörung und Servicelevel Agreement (SLA) | 8 |
| 4. Internetanschluss | 8 |
| 5. Demarkation und Eigentum | 8 |
| 6. Betrieb | 9 |
| 6.1. Softwareupdates | 9 |
| 6.2. Systemmeldungen | 9 |
| 6.3. Administration | 9 |
| 6.4. Verwaltung und Zugriffsrechte | 10 |
| 6.5. Schutzfunktion und Haftung | 10 |
| 6.6. Sicherheit der Hardware | 10 |
| 6.7. Abrechnung | 10 |
| 7. Glossar | 11 |

1. Allgemeine Informationen

ManagedFirewall ist eine Komplettlösung aus aufeinander abgestimmten Komponenten, die flexibel an die Kundenbedürfnisse angepasst werden können. Das System schützt, auf dem jeweils aktuellen Stand der Technik, die lokalen Netze und Computersysteme des Kunden vor unerwünschten Zugriffen. Die eingesetzten Systeme reduzieren damit die Sicherheitsrisiken, die bei der Verbindung lokaler Netzwerke untereinander und mit dem Internet unvermeidlich entstehen. Ein möglichst vollständiger Schutz gegen Angriffe auf Software und Hardware erfordert ein Zusammenspiel aus unterschiedlichen technischen, organisatorischen und menschlichen Komponenten und kann durch eine technische Lösung allein nicht sichergestellt werden. Die *ManagedFirewall* Komplettlösung bietet aber einen wichtigen Baustein für die individuell zu erstellende Gesamtlösung und reduziert an dieser Stelle den Aufwand durch klar definierte Serviceabgrenzung.

Die VSE NET GmbH (nachfolgend VSE NET genannt) stellt dem Kunden, im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten, eine Firewall-Lösung (*ManagedFirewall*) zur Absicherung seines Kundennetzes zur Verfügung.

ManagedFirewall beinhaltet die Bereitstellung und den Betrieb einer lokalen Firewall am Standort des Kunden. Alle durch den Kunden angeforderten Änderungen an der Firewall werden von VSE NET im Rahmen von Servicetickets durchgeführt.

ManagedFirewall muss bei mehreren Lokationen für jeden Kundenstandort einzeln beauftragt werden.

2. Technische Eigenschaften

Die nachfolgenden Aufzählungen stellen die wesentlichen technischen Eigenschaften der bereitgestellten Lösung dar. Darüber hinaus gelten die, dem Angebot beiliegenden, technischen Dokumente des Herstellers. Diese werden bei Beauftragung dieser Leistung Vertragsbestandteil.

2.1. Hardware

| Gerätebezeichnung | Empfohlen für ca. | Typischer Anwendungsbereich |
|-------------------|---------------------|--|
| FortiGate 40F | 1-10 User/Geräte | kleine Standorte mit Paketfilter, VPN und AV |
| FortiGate 60F | 10-25 User/Geräte | kleine Standorte mit Paketfilter, VPN, AV und IDS/IPS |
| FortiGate 80F | 50-100 User/Geräte | mittelgroße Standorte mit Paketfilter, VPN, AV und IDS/IPS |
| FortiGate 100F | 100-200 User/Geräte | größere Standorte mit Paketfilter, VPN, AV, IDS/IPS und SSL-Inspection |

In Abhängigkeit vom individuellen Kundenbedarf und im eigenen Ermessen von VSE NET aufgrund der technischen Rahmenbedingungen, können auch alternative Hersteller und Gerätetypen zum Einsatz kommen.

2.2. Leistungsmerkmale

Die Firewall-Systeme verfügen über umfangreiche Leistungsmerkmale. Diese sind, abhängig vom jeweils beauftragten Leistungsumfang (Service-Bundle), für den Kunden nutzbar. In den nachfolgenden Aufstellungen werden die wesentlichen Leistungsmerkmale beschrieben. Detailliertere Informationen zu den Leistungsmerkmalen können den technischen Datenblättern des Herstellers (vgl. Angebot) entnommen werden.

| Bundle | Leistungsmerkmal | Kurzbeschreibung |
|----------------------------------|---|--|
| Base Services | Basic Firewall | <p>Firewall-Grundfunktionalität</p> <p>Firewall-Regeln auf Basis von Objekten, IPs, Usern oder Endgeräten</p> <p>Vorbereitet für VPN - Verbindungen (vgl. 2.3), Logging und Monitoring (vgl. 2.4, 2.5)</p> |
| | Application Control | Signaturbasierte Erkennung einer Vielzahl von Protokolltypen, um Anwendungen gezielt zuzulassen, zu blockieren oder einzuschränken |
| | GeoIP Updates | Regelmäßige Aktualisierungen der Firewall-GeoIP-Datenbank zur Differenzierung des IP-Verkehrs anhand des geografischen Ursprungs |
| | Device/OS Detection | Erkennen von Geräten und deren Betriebssystem als Grundlage für die IPS-Funktionalität |
| | Trusted Certificate Database | Datenbank mit aktuellen Zertifikatinformationen, um SSL-Zertifikatsbrüche bzw. ungültige SSL-Zertifikate erkennen zu können |
| | Internet Service Database | Datenbank mit Informationen über häufig genutzte Internet-Services |
| Advanced Threat Protection (ATP) | Beinhaltet alle Leistungsmerkmale von Base Service zuzüglich | |
| | Intrusion Prevention System (IPS) | Erkennen und Abwehren von Bedrohungen auf Netzwerk-Ebene Umfangreiche Datenbank mit bekannten Signaturen und regelmäßigen Updates |
| | Anti-Virus | Erkennen und Abwehren von Viren in lesbaren und unverschlüsselten Datenströmen anhand bekannter Signaturen Regelmäßige Updates der Signaturdatenbank |
| | Anti-Botnet | Schutz gegen Angriffe aus bekannten Botnetzen, verhindert Kommunikation mit kompromittierten Command & Control Servern |
| | Mobile Malware | Schutz vor spezifischen Bedrohungen für mobile Endgeräte Regelmäßige Updates der Signaturdatenbank |
| | Outbreak Prevention | Erkennung von Malware-Angriffen zwischen zwei Signatur-Updates der lokalen Firewall-Datenbank Erkennung verdächtiger Daten durch Echtzeit-Abfrage von Signaturen beim Systemhersteller |
| | Inline SaaS Application Security (CASB) | Auf SaaS-Anwendungen angepasste Sicherheitsfunktionen. Erweiterte Kontrollmöglichkeiten für Netzwerkverkehr zu Cloud-Diensten (z.B. Amazon AWS, DropBox) |

| | | |
|--|---|--|
| Option: Unified Threat Protection (UTP) | Beinhaltet alle Leistungsmerkmale von Advanced Threat Protection (ATP) zuzüglich | |
| | Web and Content Filtering | Filtern von unerwünschten Webseiten und Webinhalten auf der Basis von URLs, IPs, Usern, Kategorien |
| | Secure DNS Filtering | Filtern von unsicheren DNS-Anfragen |
| | Video Filtering | Filtern von Videoinhalten in Paketströmen auf Basis von Kategorie-Filtern und/oder YouTube APIs und Parametern |
| Option: Enterprise Protection (EP) | Beinhaltet alle Leistungsmerkmale von Unified Threat Protection (UTP) zuzüglich | |
| | IT/IOT Detection and Virtual Patching Service | Erkennung und Schutz von IoT-Devices im Kundennetz Prüfung des Datenverkehrs zu erkannten IoT-Devices auf verdächtige Aktivitäten Schutz vor Angriffen auf noch ungepatchte Devices im Netz des Kunden, so, als ob bereits ein Patch auf das IoT-Device angewendet worden wäre |
| | Data Loss Prevention (DLP) | DLP ermöglicht es, Datenverluste auf Basis bestimmter Informationen (z.B. Kreditkartennummer, Kontonummer) zu erkennen und die betroffene Verbindung zu blockieren |
| | FortiConverter | Umwandeln bestehender Konfigurationen von Fremdherstellern in kompatible Konfigurationen für FortiNet. Je nach Hersteller und Konfiguration kann sich der zeitliche Aufwand im Konfigurationsworkshop verringern. |

2.3. VPN-Zugänge

Die eingesetzte Technologie ermöglicht gesicherte VPN-Verbindungen aus dem Internet (z.B. zur Anbindung von Homeoffice-Standorten) in die Netzwerke des Kunden. Es besteht die Möglichkeit, zusätzlich zur Authentifizierung mit einem Username und Passwort, eine weitere Authentifizierungsmethode zu verwenden. Die exakte Konfiguration ist abhängig vom Kundenbedarf und wird im Konfigurationsworkshop definiert. Die Nutzung der VPN-Zugänge ist mit zusätzlichen monatlichen Kosten verbunden.

2.4. FortiManager

Folgende Funktionen sind nutzbar:

- Lesender Zugriff auf Regelwerke und Objektkonfigurationen
- Lesender Zugriff auf den Systemstatus

2.5. FortiAnalyzer

Der Zugang zum FortiAnalyzer ist optional und mit zusätzlichen monatlichen Kosten verbunden.

Folgende Funktionen sind nutzbar:

- Meldung von kritischen Alarmen
- Versenden von monatlichen Status-Reports
- Übersicht über Verkehrsdaten
- Übersicht über Threats

3. Konfiguration, Installation und Abnahme

3.1. Konfigurationsworkshop

Zur Ermittlung der optimalen initialen Konfiguration der *ManagedFirewall* wird mit dem Kunden ein gemeinsamer Konfigurationsworkshop durchgeführt. Ziel des Workshops ist es, die Anforderungen des Kunden im Detail zu analysieren, zu dokumentieren und die *ManagedFirewall* optimal für den definierten Anwendungsfall einzurichten. Der Workshop ist auf eine Dauer von 4h begrenzt. Sofern diese Zeit nicht ausreicht, wird ein darüberhinausgehender Bedarf über kostenpflichtige Servicetickets abgerechnet. Sofern einzelvertraglich nicht abweichend vereinbart, findet der Workshop online statt. Findet der Workshop am Kundenstandort statt, so werden dem Kunden zusätzlich Anfahrtskosten nach den Regelungen der Dienstleistungspreisliste von VSE NET berechnet. Die Ergebnisse des Workshops werden in einem Konfigurationskatalog als Basis für die Konfiguration der *ManagedFirewall* festgehalten.

Stellt sich im Rahmen des Workshops heraus, dass vom Kunden Leistungen benötigt werden, die nicht im ursprünglichen Angebot enthalten oder technisch nicht umsetzbar sind, so behält sich VSE NET das Recht vor, das Angebot entsprechend anzupassen oder zurückzuziehen.

3.2. Konfigurationsdokumentation

Die Konfigurationsdokumentation definiert, die vom Kunden und VSE NET innerhalb des Konfigurationsworkshops erarbeiteten, initialen Einstellungen der *ManagedFirewall*. Die Konfigurationsdokumentation wird von VSE NET erstellt und dem Kunden binnen 5 Werktagen nach dem Konfigurationsworkshop zur Bestätigung bereitgestellt.

Die im Rahmen des Workshops erarbeitete Konfigurationsdokumentation muss spätestens 5 Werktage nach Übergabe an den Kunden von diesem schriftlich bestätigt und zurückgesendet werden. Ohne Übergabe dieser Bestätigung an VSE NET kann die Firewall nicht konfiguriert und nicht bereitgestellt werden.

Die Konfigurationsdokumentation stellt einen Vertragsbestandteil dar und dient als Grundlage für etwaige Anpassungen in Form von Servicetickets innerhalb der Vertragslaufzeit.

3.3. Initiale Konfiguration

Die initiale Konfiguration der Firewall erfolgt durch VSE NET auf Basis der Konfigurationsdokumentation. Konfiguration und Inbetriebnahme der Firewall sind ohne schriftlich bestätigte Konfigurationsdokumentation nicht möglich.

3.4. Installation

Die Installation wird durch einen Techniker von VSE NET oder durch einen von VSE NET beauftragten Dienstleister zusammen mit dem technischen Ansprechpartner des Kunden vorgenommen. Sie erfolgt in enger Abstimmung mit dem Kunden, um Ausfallzeiten so kurz wie möglich zu halten. Der technische Ansprechpartner ist im Rahmen des vorbereitenden Konfigurationsworkshops (vgl. 3.1) vom Kunden zu benennen.

3.5. Abnahme

Die Systemkonfiguration zum Zeitpunkt der Installation wird durch ein schriftliches Abnahmeprotoll dokumentiert und von einem dazu berechtigten Ansprechpartner des Kunden sowie durch einen Ansprechpartner von VSE NET unterschrieben. Nach Unterzeichnung der Abnahme ist die *ManagedFirewall* für den Betrieb im Managed Service freigegeben. Ab diesem Zeitpunkt sind Änderungen der Konfiguration ausschließlich durch explizite Beauftragung durch den Kunden über Servicetickets möglich.

3.6. Einweisung

Der Kunde erhält eine Einweisung in den FortiManager sowie in die Analysefunktionen des FortiAnalyzer, sofern diese mit beauftragt wurden. Diese Einweisung findet, sofern nicht einzelvertraglich abweichend vereinbart, online statt. Die Einweisung ist auf die Dauer von 2h begrenzt. Sofern diese Zeit nicht ausreicht, wird die darüberhinausgehende Zeit über Servicetickets abgerechnet.

3.7. Entstörung und Servicelevel Agreement (SLA)

VSE NET bearbeitet Servicetickets und Störungstickets des Kunden im Rahmen der technischen und betrieblichen Möglichkeiten. Es gelten die Bestimmungen des Dokuments [SLA_ManagedFirewall](#).

4. Internetanschluss

Dieses Angebot beinhaltet keinen Internetanschluss. *ManagedFirewall* setzt eine Internetverbindung voraus, die über VSE NET oder einen anderen Anbieter bezogen werden kann. Bei der Nutzung von Internetanschlüssen anderer Anbieter gelten für *ManagedFirewall* Einschränkungen bzgl. Servicequalität und den möglichen Reaktionszeiten bei Störungen (vgl. Dokument [SLA_ManagedFirewall](#)).

5. Demarkation und Eigentum

Der Dienst *ManagedFirewall* wird dem Kunden an einem oder mehreren elektrischen oder optischen Ethernet-LAN-Ports der von VSE NET bereitgestellten Firewall übergeben. Für Betrieb, korrekte Funktion und die Sicherheit der an diese Ports angeschlossenen Systeme (z.B. Router, Switches, PCs, Drucker, WLAN-Access-Points, sonstige Netzwerkkomponenten) ist ausschließlich der Kunde verantwortlich. VSE NET übernimmt aus diesem Vertragsverhältnis heraus zu keinem Zeitpunkt administrative Tätigkeiten auf den Systemen des Kunden. Störungen, die ihre Ursache im Verantwortungsbereich des Kunden haben, werden bei der Einhaltung der zugesagten SLA-Parameter nicht berücksichtigt (vgl. [SLA_ManagedFirewall](#)).

Die von VSE NET zur Bereitstellung des Dienstes eingesetzte Hardware verbleibt im Eigentum von VSE NET und geht nicht in das Eigentum des Kunden über. Nach Vertragsende muss die Hardware innerhalb von 14 Werktagen vom Kunden frei Haus an VSE NET zurückgesendet werden. Wird die Rücksendung versäumt, so ist VSE NET berechtigt, dem Kunden die Hardware auf Basis des Zeitwerts, mindestens jedoch aber 250€, in Rechnung zu stellen.

6. Betrieb

VSE NET stellt im Rahmen von *ManagedFirewall* den grundlegenden Betrieb der Firewall, des zentralen Managements (FortiManager) sowie, falls durch den Kunden beauftragt, des Analysetools (FortiAnalyzer) sicher.

Dazu zählen:

- Installation und Inbetriebnahme der Firewall am Kundenstandort
- Betrieb, Entstörung und Überwachung von FortiManager und FortiAnalyzer
- Erreichbarkeit der Firewall über die Internetverbindung (bei Internetanschlüssen von VSE NET)
- Installation von Updates, Patches und Fixes nach den Herstellervorgaben
- Life-Cycle Management durch Tausch und Entstörung der bereitgestellten Firewall
- Backup und Sicherung der Konfiguration

Der Betrieb erfolgt auf Basis der vereinbarten SLA-Bedingungen (vgl. Dokument *SLA_ManagedFirewall*).

6.1. Softwareupdates

VSE NET übernimmt die regelmäßige Aktualisierung der Software aller Komponenten (FortiGate Firewall, FortiManager, FortiAnalyzer) nach den Vorgaben des Systemherstellers. Durch die Softwareupdates wird sichergestellt, dass alle Komponenten auf einem aktuellen und sicheren Stand gehalten werden. Sofern die verwendete Firewall-Hardware einen weiteren Betrieb nicht mehr gewährleistet (End-of-Life), wird durch VSE NET ein neues Endgerät bereitgestellt. Die Softwareupdates erfolgen nach den Bestimmungen des Service Level Agreement (*SLA_ManagedFirewall*).

6.2. Systemmeldungen

VSE NET sendet automatisiert sicherheitsrelevante Systemmeldungen an im Konfigurationsworkshop verbindlich festgelegte E-Mail-Adressen des Kunden oder an die eines durch den Kunden beauftragten Dienstleisters. Diese Informationen werden systematisch kategorisiert und entsprechend der Kritikalität eingestuft. Meldungen ab der Kritikalität "warning" werden an die hinterlegte(n) E-Mail-Adresse(n) des Kunden und an das Network Operation Center von VSE NET versendet. Diese Meldungen umfassen mögliche Angriffe sowie kritische Systemzustände. Eine Anpassung der Konfiguration der Meldekette und der festgelegten Alarme wird im Konfigurationsworkshop vorgenommen.

Der Kunde ist dafür verantwortlich Änderungen der E-Mail-Adresse(n) unverzüglich an VSE NET zu kommunizieren. Das gilt insbesondere bei dem Ausscheiden eines Mitarbeiters oder bei Wechsel des vom Kunden beauftragten Dienstleisters. Die Kommunikation muss über den im Angebot benannten Vertriebskontakt von VSE NET erfolgen. Eine Änderung der E-Mail-Adressen per Service-Ticket ist aus Sicherheitsgründen nicht möglich.

6.3. Administration

Die Administration der Firewall Einstellungen erfolgt ausschließlich durch VSE NET. Die vom Kunden beauftragten Änderungen werden im Rahmen von Servicetickets (vgl. Dokument *SLA_ManagedFirewall*) bearbeitet und abgerechnet. Alle erforderlichen Maßnahmen bezüglich des Betriebs und Änderungen der Systemkonfiguration werden von VSE NET in Abstimmung mit dem Kunden vorgenommen. Die Durchführung von Änderungen wird anhand von Servicetickets dokumentiert und abgerechnet.

6.4. Verwaltung und Zugriffsrechte

Der Kunde erhält, bei entsprechender Beauftragung, sowohl für den FortiManager als auch für den FortiAnalyzer, ausschließlich Zugänge mit Leseberechtigung, da sämtliche Konfigurationsmaßnahmen auf den genannten Systemen von VSE NET durchgeführt werden. Die Zugriffsrechte ermöglichen die Anzeige von Netzwerkeinstellungen, Firewall Regeln, Logdateien und Analysefunktionen. Sofern nicht einzelvertraglich abweichend vereinbart, ist im monatlichen Grundpreis ein Zugang für den FortiManager enthalten. Weitere Zugänge sind kostenpflichtig und können optional beauftragt werden. Es sind maximal je drei Zugänge für FortiManager und FortiAnalyzer möglich.

6.5. Schutzfunktion und Haftung

Die mit der Nutzung des Internets verbundenen Gefahren und die sich hierdurch für die Kundenumgebung ergebenden Sicherheitsrisiken sind sehr vielfältig und unterliegen einer laufenden Änderung und Weiterentwicklung. Der in diesem Dokument beschriebene Dienst wird von VSE NET auf Basis der Hard- und Software des Herstellers Fortinet erbracht. Die IP-Netzwerke des Kunden sind durch den Dienst, nach dem jeweils technisch möglichen Stand des Herstellers, bestmöglich geschützt. Es ist, wie bei allen technischen Systemen, nicht möglich, einen vollständigen Schutz gegen alle denkbaren Angriffsszenarien zu erreichen. VSE NET erbringt die vereinbarte Leistung, insbesondere die Softwareupdates und das Patchen von durch den Hersteller an VSE NET kommunizierten Sicherheitslücken. VSE NET übernimmt für die Folgen von Angriffen und Fehlfunktionen, die durch z.B. noch unentdeckte Sicherheitslücken der Soft- und Hardware oder durch Angriffe, die von den Systemen nicht erkannt werden, entstehen keine Haftung.

6.6. Sicherheit der Hardware

Die beim Kunden vor Ort eingesetzten Geräte müssen jederzeit gemäß den vom Hersteller beschriebenen technischen Spezifikationen (vgl. Datenblätter der Geräte) betrieben werden. Dies gilt insbesondere für die elektrischen und optischen Anschlüsse, die Installationsart sowie die Betriebsumgebung. Der Kunde ist für die Einhaltung dieser Bedingungen verantwortlich und sorgt auf eigene Rechnung dafür, dass die gesetzlich vorgeschriebene, wiederkehrende DGUV-Prüfung vorgenommen wird. VSE NET wirkt bei einer erforderlichen Abschaltung (Wartungsmaßnahme) nach Vereinbarung und Eröffnung eines Servicetickets mit. VSE NET haftet ausdrücklich nicht für Schäden, die durch unsachgemäßen Betrieb entstehen. Vom Kunden festgestellte Mängel an Geräten, die von VSE NET an seinem Standort betrieben werden, sind VSE NET unverzüglich durch Eröffnung eines Störungstickets zu melden.

6.7. Abrechnung

VSE NET berechnet, in Abhängigkeit von der konkret beauftragten Konfiguration der Systemkomponenten, für *ManagedFirewall* eine einmalige Einrichtungspauschale und eine monatliche Grundgebühr. Optionale Leistungen werden separat abgerechnet. Sofern vertraglich nicht abweichend vereinbart, gelten die im Angebot fixierten Preise für *ManagedFirewall* sowie die Dienstleistungspreisliste der VSE NET. Servicetickets werden nach den Regelungen des Dokuments *SLA_ManagedFirewall* und auf Basis der Dienstleistungspreisliste der VSE NET abgerechnet.

7. Glossar

| Abkürzung | Kurzbeschreibung |
|---|---|
| VPN Virtuelles Privates Netz | Verbindungen vom Home-Office zur Zentrale oder zwischen zwei Kundenstandorten. Die Verbindung wird dabei verschlüsselt über das Internet aufgebaut. |
| AV Antivirus | Antivirus Schutz der Kundeninfrastruktur vor bekannten Viren. |
| IDS Intrusion Detection System | Ein Intrusion Detection System (IDS) ist eine Anwendung, die den Netzwerkverkehr überwacht und nach bekannten Bedrohungen sowie verdächtigen oder böswilligen Aktivitäten sucht. Das IDS sendet Warnungen, wenn es Sicherheitsrisiken und -bedrohungen erkennt. |
| IPS Intrusion Prevention System | Das Intrusion Prevention System (IPS) ist ein Element der Firewall das ein Netzwerk kontinuierlich auf böartige Aktivitäten überwacht und Maßnahmen ergreift, um diese zu verhindern, einschließlich der Meldung, Blockierung oder Löschung, wenn sie auftreten und durch das IDS erkannt werden. |
| SSL-Inspection | Zur Sicherung des Datenverkehrs wird SSL-Verschlüsselung (z.B. beim Homebanking) verwendet. Der verschlüsselte Datenverkehr kann jedoch dazu verwendet werden, die normalen Abwehrmaßnahmen Ihres Netzwerks zu umgehen. Mithilfe der SSL/TLS-Tiefenprüfung können Firewalls den Datenverkehr auch dann prüfen, wenn er verschlüsselt ist. |