Managed Firewall

Leistungsbeschreibung

***Effizienterer Betrieb**, **schnelleres Wachstum** und **mehr Leistung** für Ihre*

INHALTSVERZEICHNIS

1 Einführung

Dieses Dokument beschreibt den Managed-Firewall-Service von Ingram Micro (nachfolgend Ingram Micro).

Dank unserer flexiblen Managed Services können unsere Kunden frei entscheiden, ob sie die IT-Umgebung ihrer Kunden ganz oder in Teilen durch das Network Operating Center (NOC) von Ingram Micro verwalten lassen möchten. Unser Network Operating Center bietet alle Funktionen und Vorteile einer eigenen IT-Abteilung, ohne dass Sie oder Ihre Kunden sich selbst um Wissensmanagement, Ressourcenbeschaffung oder spezielle NOC-Lösungen kümmern müssen. Die erfahrenen IT-Experten in unserem NOC bieten proaktives Management und Remote-Unterstützung.

1.1 MANAGED FIREWALL AUF EINEN BLICK

Managed Firewall ist ein Managed Service von Ingram Micro zur Verwaltung von Firewall-Infrastruktur.
Der Leistungsumfang wird in diesem Dokument detailliert beschrieben.

Ingram Micro bietet Managed Firewall in zwei Varianten an:

1. Managed Firewall ***Basic*** – Alle Services von Ingram Micro werden auf Service-Level Standard erbracht. In der Variante „Basic“ werden Überwachungstools des Anbieters für die Netzwerkverwaltung eingesetzt.

2. Managed Firewall ***Standard*** – Alle Services von Ingram Micro werden auf Service-Level Standard erbracht. In der Variante „Standard“ wird die Überwachungssoftware Auvik für die Netzwerkverwaltung eingesetzt. Auvik ist eine professionelle Überwachungsplattform für Netzwerkumgebungen auf Enterprise-Ebene. Die Überwachung ist deutlich umfassender als in der Variante „Basic“.

Die Leistungsbeschreibung für Managed Firewall beruht auf folgenden Komponenten:

- Unterstützte Funktionen
- Hardware
- Überwachung und Reaktion
- Patch- und Versionsverwaltung
- Backup und Wiederherstellung
- Leistungskriterien und Berichterstattung

2 Managed Firewall

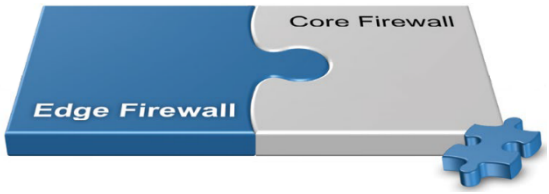
Dieses Kapitel beschreibt die Zwecke und Funktionen der verschiedenen Komponenten des Managed-Firewall-Service von Ingram Micro. In Anlage 1 finden Sie eine Zusammenfassung aller Funktionen und Inhalte des Service.

2.1 UNTERSTÜTZTE FUNKTIONEN

Der Managed-Firewall-Service unterstützt zahlreiche verschiedene Funktionen. Innerhalb des Service wird zwischen Managed Firewall Standard und Managed Firewall Tailor-Made unterschieden.

Folgende Funktionen werden durch den Managed-Firewall-Service unterstützt:

1. Edge-Firewall
2. Core-Firewall
3. SSL-Verbindungen
4. IPsec-Verbindungen
5. Filterung von Webinhalten
6. Intrusion Prevention
7. Antivirus
8. Antispam



Nutzungs- und Funktionsumfang dieser Optionen unterscheiden sich zwischen den Servicemodellen Standard und Tailor-Made.

2.1.1 Edge-Firewall

Edge-Firewalls befinden sich am äußeren Perimeter eines Netzwerks, wo Verbindungen nach außen, beispielsweise ins Internet, anliegen. Ein typisches Beispiel sind Firewalls an Bürostandorten, die sichere Verbindungen nach außen benötigen. Hier greifen verschiedene Sicherheitsfunktionen. Die verfügbare Funktionalität unterscheidet sich nach Hersteller, Modell und erworbenen Lizenzen.

Im Rahmen unseres Service wird zwischen zwei Arten von Edge-Firewalls unterschieden: nach Endnutzern oder nach Bandbreitennutzung.

Die kleinere Variante Edge 1 ist für Umgebungen mit weniger als 25 Endnutzern gleichzeitig und/oder weniger als 20 Mbit/s Bandbreite.

Die Firewall Edge 2 ist für Umgebungen mit mehr als 25 gleichzeitigen Nutzern oder mehr als 20 Mbit/s genutzter Bandbreite.

Die Edge-Firewall-Funktion steht in den Serviceversionen „Basic“ und „Standard“ zur Verfügung.

2.1.2 Core-Firewall

Firewalls im Zentrum des Netzwerks sind kritische Komponenten der Netzwerkstruktur. Dazu gehören zum Beispiel zentrale Firewall-Umgebungen in Rechenzentren. Ihre Position ermöglicht die Überwachung und Kontrolle des gesamten Datenverkehrs im Netzwerk. Sämtlicher Traffic geht über die Firewall und wird von ihr nach unerwünschtem Verhalten gescannt.

Die Core-Firewall-Funktion steht in der Serviceversion „Standard“ zur Verfügung.

2.1.3 SSL-Verbindungen

SSL-Verbindungen sind geschützte Verbindungen, über die Mitarbeiter oder externe Personen sicher auf IT-Services und/oder -Infrastruktur zugreifen können. Eine solche sichere SSL-Verbindung wird mittels Software (SSL-Client) hergestellt. Für noch mehr Schutz können persönliche Tokens genutzt werden. Diese generieren einen Einmalcode, der zusätzlich zu Benutzername und Passwort eingegeben werden muss. Die Nutzung und Verwaltung solcher Tokens ist nicht Teil des Service.

Die Verwaltung der SSL-Funktion wird in den Serviceversionen „Basic“ und „Standard“ angeboten.

2.1.4 IPsec-Verbindungen

IPsec-Verbindungen sind direkte Verbindungen zwischen Standorten zum Zweck der sicheren Kommunikation. Firewalls bieten meist die Möglichkeit, mehrere solche Verbindungen aufzubauen. Auch der darüber laufende Datenverkehr kann von der Firewall auf unerwünschte Verhaltensweisen und Inhalte überprüft werden.

Ingram Micro übernimmt die Einrichtung und Überwachung der IPsec-Verbindungen auf den im Vertrag festgelegten Firewalls. Muss eine IPsec-Verbindung zu einer Firewall aufgebaut werden, die von einem Drittanbieter und/oder Kunden verwaltet wird, obliegt die Verantwortung für die Einrichtung der Verbindung dem Drittanbieter und/oder Kunden.

Die Verwaltung der IPsec-Verbindungen wird in den Serviceversionen „Basic“ und „Standard“ angeboten.

2.1.5 Filterung von Webinhalten

Die Filterung von Webinhalten ist eine Firewall-Funktion, die Inhalte von Websites ständig auf unerwünschtes Verhalten überprüft. So werden Endnutzer bestmöglich gegen schädliche Aktionen auf Websites geschützt. Unsichere oder unerwünschte Inhalte werden blockiert. Die Verwaltung der Funktion und der entsprechenden Richtlinien ist Teil des Service. Die Firewall muss die Funktion unterstützen. Der Erwerb entsprechender Lizenzen für die Firewall liegt in der Verantwortung des Kunden.

Die Filterung von Webinhalten wird in den Serviceversionen „Basic“ und „Standard“ unterstützt.

2.1.6 Intrusion Prevention

Viele Organisationen speichern ihre Daten in öffentlichen oder privaten Clouds oder in Rechenzentren. Nur berechtigte Mitarbeiter dürfen auf diese Daten zugreifen. Intrusion Prevention ist ein Mechanismus, der das kontrolliert und sicherstellt. Die Funktion erkennt häufig von Hackern genutzte Methoden und erschwert so den unbefugten Zugriff auf Daten.

Die Firewall muss die Funktion unterstützen. Der Erwerb entsprechender Lizenzen für die Firewall liegt in der Verantwortung des Kunden. Intrusion Prevention wird in den Serviceversionen „Basic“ und „Standard“ unterstützt.

2.1.7 Antivirus

Die Antivirusfunktion scannt den Datenverkehr auf bösartige Verhaltensweisen und Schaddaten. Werden Daten als Virus erkannt, greift der Mechanismus ein und blockiert sie. Die Firewall muss die Funktion unterstützen. Der Erwerb entsprechender Lizenzen für die Firewall liegt in der Verantwortung des Kunden. Antivirus wird in den Serviceversionen „Basic“ und „Standard“ unterstützt.

2.1.8 Antispam

Die Nutzung dieser Funktion schützt bestmöglich vor Phishing-Versuchen und unerwünschter Werbung. Die Firewall muss die Funktion unterstützen. Der Erwerb entsprechender Lizenzen für die Firewall liegt in der Verantwortung des Kunden. Antispam wird in den Serviceversionen „Basic“ und „Standard“ unterstützt.

2.2 HARDWARE

2.2.1 Unterstützte Marken

Ingram Micro unterstützt sämtliche Firewall-Hardware, die unter das Geschäftssegment seiner Services fällt und remote verwaltet werden kann. Um einen hochwertigen Service zu garantieren, behält Ingram Micro sich vor, Geräte auszuschließen, für die keine ordnungsgemäße Verwaltung möglich ist.

Ingram Micro kann höherwertige oder umfangreichere Dienstleistungen anbieten, wenn die Variante „Basic“ oder „Standard“ im Bereich Firewall-Hardware ausgewählt wird. Ingram Micro führt standardmäßig die Netzwerkserien Fortinet, Cisco Enterprise und Cisco Meraki. Alle Network Consultants und Network Engineers sind dafür ausgebildet und zertifiziert.

Für Geräte der Marke Cisco Meraki gilt die Serviceversion *Managed Firewall Basic*; für Geräte der Marken Fortinet und Cisco gilt die Version *Managed Firewall Standard*.

2.2.2 Rücksendung (RMA) und Ersatz

Sowohl bei *Managed Firewall Basic* als auch bei *Managed Firewall Standard* kümmert sich Ingram Micro um die gesamte RMA-Abwicklung für defekte Hardware. Nach der Meldung beschädigter oder defekter Hardware übernimmt Ingram Micro den kompletten RMA-Prozess gegenüber Fortinet oder Cisco/Meraki.

Der Austausch der Hardware vor Ort wird gemäß Nachkalkulation abgerechnet. Der Kunde kann sich auch entscheiden, die Hardware selbst zu ersetzen. Ingram Micro behält jederzeit die Koordination des RMA-Prozesses inne.

Ist das zu ersetzende Gerät in einer gewissen Höhe angebracht, wird ein Drittunternehmen hinzugezogen. Dies dient der Sicherheit unserer Mitarbeiter. Die anfallenden Kosten werden gemäß Nachkalkulation abgerechnet.

Ein Hardware-Supportvertrag mit dem Hersteller ist eine der grundlegenden Konditionen unserer Services.

2.2.3 Architektur und Beratung

Mit *Managed Firewall Basic* und *Managed Firewall Standard* können Sie Fragen der Architektur und die Beratung zu Ersatzhardware uns überlassen. So können Sie als Kunde alles an ein Unternehmen outsourcen und müssen keine eigenen Ressourcen oder Drittanbieter dafür einsetzen. Voraussetzung ist, dass die Hardware von Fortinet, Cisco oder Cisco Meraki stammt.

Architektur und Beratung ist eine Zusatzoption für die Serviceversion „Basic“. In der Version „Standard“ ist diese Komponente enthalten.

2.2.4 Kabel und Peripheriegeräte

Ingram Micro kann auch die Installation und den Austausch von Kabeln und Peripheriegeräten für Sie übernehmen. Dies umfasst physische Kabel, Patchschränke, Kabelkanäle und Konfektionierung. Diese Dienstleistung wird mithilfe eines Partners von Ingram Micro erbracht. Ingram Micro behält jederzeit die Koordination inne. Die anfallenden Kosten werden gemäß Nachkalkulation abgerechnet.

2.3 ÜBERWACHUNG UND REAKTION

Das Network Operating Center oder NOC von Ingram Micro ist für die Überwachung und Verwaltung der Netzwerkumgebung zuständig.

Die Netzwerküberwachung erfolgt in der Serviceversion „Basic“ mithilfe der Standardüberwachungssoftware des entsprechenden Herstellers/Anbieters und in der Version „Standard“ mittels unseres hochwertigen Netzwerküberwachungstools Auvik. Beide Varianten nutzen zudem die Erfahrung unserer spezialisierten Netzwerkadministratoren und Network Consultants.

Die eingesetzte Überwachungssoftware Auvik wurde speziell für die Verwaltung von Netzwerkinfrastrukturen entwickelt. Sie bietet nicht nur Einblicke in die Netzwerkinfrastruktur, sondern zeigt Ingram Micro auch die mit dem Netzwerk verbundenen Geräte. So können alle Geräte, die über eine IP-Adresse mit dem Netzwerk verbunden sind, überwacht werden.

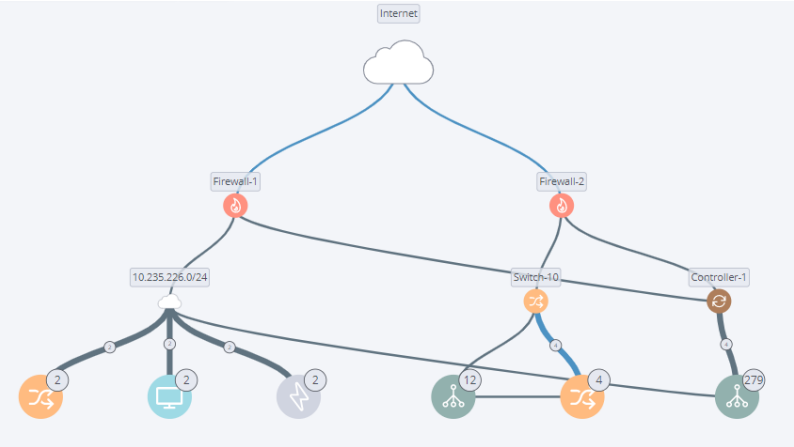


Abbildung 1: Beispielhafte Visualisierung einer physischen Netzwerkhierarchie in Auvik

Ingram Micro misst die folgenden Kennwerte:

1. Verfügbarkeit
2. Auslastung
3. Bandbreite und Traffic

Alarmierung
Die Überwachungssoftware sendet anhand festgelegter Parameter Alarme, auf die das NOC umgehend und gemäß den SLA-Vereinbarungen reagiert. Das System nimmt automatisch eine Klassifizierung nach Art und Schweregrad des Fehlers vor. Das NOC von Ingram Micro legt dann anhand der spezifischen Kundensituation (Geschäftsauswirkungen) die Priorität der Vorfallsbehandlung fest. Dies erfolgt immer in Abstimmung mit dem Kunden. Schon das Versagen einer einzelnen Firewall kann schwere Auswirkungen auf den Geschäftsbetrieb haben. Weitere Informationen zur Priorisierung von Vorfällen finden Sie im Service Level Agreement (SLA) von Ingram Micro.

Datenvorhaltefristen
Die Überwachungs- und Konfigurationsdaten der Systeme werden gemäß dem aktuellen Vertrag für maximal 10 Jahre gespeichert. Läuft der Vertrag aus oder wird gekündigt, löscht Ingram Micro die Überwachungsdaten dauerhaft aus allen Systemen.

2.3.1 Verfügbarkeit

Die wichtigste Kenngröße der Überwachung ist die Netzwerkverfügbarkeit. Die Verfügbarkeit hängt von verschiedenen Faktoren innerhalb des Netzwerks ab. In Kombination entscheiden diese darüber, ob der Service verfügbar ist oder nicht. Ingram Micro überwacht die Verfügbarkeit jedes Netzwerkgeräts, um die Gesamtverfügbarkeit zu messen.

Die Verfügbarkeit der folgenden Komponenten wird ständig überprüft:

- Hardwaregeräte
- Ports und Verbindungen
- Administrative Konfiguration
- Betriebskonfiguration
- Backup
- Anmeldung
- SNMP

Die Verfügbarkeit ist der wichtigste Parameter des Service. Für jedes Quartal wird ein Bericht zur Hardwareverfügbarkeit erstellt.

2.3.2 Auslastung

Die Auslastung oder Nutzung der verfügbaren Ressourcen wird ebenfalls ständig gemessen; einerseits, um die Verfügbarkeit sicherzustellen, aber insbesondere, um Muster zu erkennen und Probleme angemessen analysieren zu können.

Die folgenden Auslastungsparameter werden erfasst:

- Prozessorauslastung in %
- Arbeitsspeicherauslastung in %
- Speicher in % (gegebenenfalls)
- Portnutzung in %

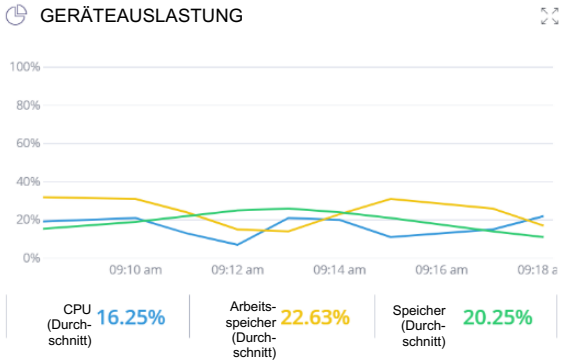


Abbildung 2: Beispielhafte Geräteauslastung

2.3.3 Bandbreite und Traffic

Der gesamte Datenverkehr, der über die Managed-Firewall-Hardware läuft, wird durch die Systeme von Ingram Micro oder den Hersteller kontinuierlich gemessen.

Nur in der Version „Standard“ werden die folgenden Parameter ständig proaktiv gemessen:

- Bandbreite pro Gerät – durchschnittliche Mbit/s
- Bandbreite pro Schnittstelle – durchschnittliche Mbit/s
- Datenpakete pro Gerät – durchschnittliche Anzahl pro Sekunde
- Datenpakete pro Interface – durchschnittliche Anzahl pro Sekunde
- Datenpaketverlust pro Interface – durchschnittliche Anzahl pro Sekunde

Das Verhalten des Traffics wird ständig überwacht und bei inkonsistenten Änderungen laut System werden Alarme gemäß den erwarteten Auswirkungen ausgelöst.

Zertifikatsverwaltung, Überwachung für mehrere Hersteller sowie die Plattform und die Lernfunktion für die Intelligente Überwachung sind nur in der Version „Standard“ enthalten.

2.4 PATCH- UND VERSIONSVERWALTUNG

Um die Sicherheit und Funktionalität des Netzwerks zu gewährleisten, muss die Firmware auf der Firewall-Hardware aktuell gehalten werden.

Dabei unterscheidet Ingram Micro zwischen folgenden Update-Arten:

1. Sicherheitspatches
2. Funktionsupdates

Sowohl bei *Managed Firewall Basic* als auch bei *Managed Firewall Standard* sind Sicherheitspatches, Sicherheitsupdates und Funktionsupdates Teil der Leistung.

2.4.1 Sicherheitspatches

Sicherheitspatches werden von den Hardwareherstellern veröffentlicht, um Schwachstellen und Bugs zu beheben. Bei *Managed Firewall Basic* und *Managed Firewall Standard* überwacht Ingram Micro die gesamte Firewall-Hardware und prüft, ob erforderliche Patches verfügbar sind. Ingram Micro installiert die vom Hersteller als erforderlich eingestuften Sicherheitspatches, um die Sicherheit und Verfügbarkeit zu gewährleisten. Für die Installation von Sicherheitspatches wird der Change-Management-Prozess gestartet, um der Netzwerkhardware die benötigte Firmware bereitzustellen.

2.4.2 Funktionsupdates

Hersteller von Netzwerkgeräten veröffentlichen regelmäßig neue Funktionen für ihre Netzwerkhardware. Ingram Micro bezeichnet diese Updates als Funktionsupdates. Funktionsupdates erfolgen immer als nicht standardmäßige Änderungen und sind Teil des Service bei *Managed Firewall Basic* und *Managed Firewall Standard*. Funktionsupdates werden nur auf Kundenanfrage oder nach Empfehlung durch Ingram Micro ausgeführt.

2.4.3 Wartungsfenster

Bei Managed Firewall Basic und Managed Firewall Standard erfolgt die proaktive Wartung angesichts der geschäftskritischen Natur der Servicebereitstellung in Absprache mit dem Kunden.

2.5 BACKUP UND WIEDERHERSTELLUNG

Sämtliche von Ingram Micro im Rahmen des Managed-Firewall-Service verwaltete Firewall-Hardware ist von unserem Backup-Service abgedeckt. Diese Funktion ist in beiden Serviceversionen, „Basic“ und „Standard“, enthalten, ausgenommen der Export von Gerätekonfigurationen und die Speicherung der Konfigurationshistorie. Diese Funktionen sind nur in der Version „Standard“ verfügbar.

2.5.1 Backup

Jede von Ingram Micro verwaltete Firewall-Hardware wird automatisch gesichert. Alle Änderungen an einem Gerät werden automatisch im Service gespeichert.

Neben dem automatischen Backup der Hardware werden alle Konfigurationen unbegrenzt gespeichert. Mit dieser Funktion können Sie jederzeit alte Konfigurationen ansehen und Konfigurationen miteinander vergleichen. Auch bei beispielsweise erfolglosen Change Requests externer Parteien kann die letzte funktionierende Konfiguration schnell und einfach wieder hergestellt werden.

Die Backup-Funktion kann bereitgestellt werden, wenn die Firewall durch die Managementsoftware von Ingram Micro unterstützt wird und der Remote-Zugriff per SSH-Protokoll möglich ist. Das Telnet-Protokoll wird nicht unterstützt.

Ist mindestens eine dieser Bedingungen nicht erfüllt, kann Ingram Micro die Sicherung der Firewall-Hardware nicht garantieren.

2.5.2 Wiederherstellung

Die Wiederherstellung einer gesicherten Konfiguration eines Netzwerkgeräts ist standardmäßig Teil des Service. Dies ist unter anderem bei menschlichem Versagen oder beim Austausch eines Firewall-Geräts notwendig.

Um die Kontinuität sicherzustellen, erfolgt die Wiederherstellung einer Konfiguration immer unter Aufsicht von und durch Ingram Micro. Wurde die Konfiguration aus irgendeinem Grund durch Dritte geändert, wird die Wiederherstellung des Backups immer gemäß Nachkalkulation abgerechnet.

2.5.3 Export von Konfigurationen

Bei der Serviceversion *Managed Firewall Standard* kann der Export der Konfiguration eines oder mehrerer Netzwerkgeräte angefordert werden. Die anfallenden Kosten werden gemäß Nachkalkulation abgerechnet.

3 Leistungskriterien

Die allgemeinen Leistungskriterien von Ingram Micro sind im Service Level Agreement (SLA) beschrieben. Die Leistungsbeschreibung benennt, welche Punkte spezifisch für den Managed-Firewall-Service gelten.

3.1 SERVICEZEITEN

Für den Managed-Firewall-Service sind zwei Arten von Servicezeiten verfügbar:

- Geschäftszeiten
- Prio-1-Support rund um die Uhr

Der Prio-1-Support rund um die Uhr ist optional verfügbar und wird über alle im Servicevertrag festgelegten Firewall-Geräte berechnet.

3.2 KONFIGURATIONSMANAGEMENT

Ingram Micro ist für die folgenden Konfigurationselemente aller von Ingram Micro verwalteten Geräte verantwortlich:

Konfigurationselemente*		
Gerätename	Seriennummer	Platte(n) (gegebenenfalls)
Gerätetyp	Firmware-Version	Arbeitsspeicher
IP-Adressen	VPN-Tunnel	Netzwerkschnittstellen
Netzwerke	Benutzernamen	
Marke	Passwörter	
Modell	Cluster-/Stack-Konfiguration	
Software-Version	CPU(s)	

** Wenn Geräte nicht über ein oder mehrere Konfigurationselemente verfügen oder nicht ausgelesen werden können, werden diese Konfigurationen nicht von Ingram Micro gepflegt.*

3.3 BERICHTERSTATTUNG

3.3.1 Portal

Folgende Komponenten kann der Kunde über das Portal einsehen:

1. Verfügbarkeit
2. Vorfallsübersicht und Kennzahlen
3. Änderungsübersicht und Kennzahlen

3.3.2 Trendanalysen und Empfehlungen

Bei der Serviceversion *Managed Firewall Standard* wird einmal pro Quartal eine Trendanalyse mit relevanten Empfehlungen erstellt. Die Trendanalyse und die Empfehlungen werden persönlich mit dem Kunden besprochen, um den Service für Ingram Micro, den Kunden und eventuelle Dritte zu optimieren.

Die Trendanalysen und Empfehlungen sind nur bei *Managed Firewall Standard* enthalten.

4 Geschäftsbedingungen

4.1 URHEBERRECHT

Diese Leistungsbeschreibung darf ohne vorherige schriftliche Genehmigung von Ingram Micro weder vollständig noch in Auszügen mittels Druck, Offsetdruck, Fotokopie oder Mikrofilm oder in irgendeiner digitalen, elektronischen, optischen oder sonstigen Form vervielfältigt oder veröffentlicht werden oder (dies gilt gegebenenfalls zusätzlich zum Urheberrecht) zum Vorteil eines Unternehmens, einer Organisation oder eines Instituts oder zur persönlichen Nutzung oder Lektüre vervielfältigt werden.

4.2 HAFTUNGSAUSSCHLUSS

Bei der Erstellung dieser Leistungsbeschreibung wurde höchste Sorgfalt auf die Richtigkeit der enthaltenen Informationen verwendet. Dennoch ist Ingram Micro nicht für in dieser Leistungsbeschreibung enthaltene Fehlinformationen verantwortlich.

4.3 ALLGEMEINE GESCHÄFTSBEDINGUNGEN

Die Dienstleistungen werden gemäß den beim Bezirksgericht Midden-Nederland am Standort Utrecht hinterlegten Geschäftsbedingungen von NLdigital erbracht, die über unsere Website eingesehen werden können.

Zusätzlich zu den Allgemeine Geschäftsbedingungen von Ingram Micro B.V. gelten die vertraglichen Geschäftsbedingungen in der geschlossen Vereinbarung.

4.4 KONTAKTDATEN INGRAM MICRO

Ingram Micro B.V.
Papendorpseweg 95
3528 BJ Utrecht
Tel.: +31 (0) 30 246 40 01

5 Anlage 1: Servicerubrik

MANAGED FIREWALL

√ Enthalten

O Optional/nicht standardmäßige Änderung

- Nicht möglich/nicht anwendbar

	BASIC		STANDARD	
UNTERSTÜTZTE FUNKTIONEN	Edge	Core	Edge	Core
Edge-Firewall	√	*nicht anwendbar*	√	-
Core-Firewall/Routing	√	*nicht anwendbar*	-	√
SSL-Verbindungen	√	*nicht anwendbar*	√	√
IPsec-Verbindungen	√	*nicht anwendbar*	√	-
Inhaltsfilterung(1)	√	*nicht anwendbar*	√	√
Intrusion Prevention(1)	√	*nicht anwendbar*	√	√
Antivirus(1)	√	*nicht anwendbar*	√	√
Antispam(1)	√	*nicht anwendbar*	√	√
HARDWARE				
Unterstützte Marken (2)	Cisco Meraki	Cisco Meraki	Cisco ASA und Fortinet	Cisco ASA und Fortinet
RMA und Ersatz (3) (4)	√	*nicht anwendbar*	√	√
Architektur und Beratung	O	*nicht anwendbar*	√	√
Kabel und Peripheriegeräte	O	*nicht anwendbar*	O	O
ÜBERWACHUNG UND REAKTION				
Verfügbarkeit	√	*nicht anwendbar*	√	√
Auslastung/Nutzung	√	*nicht anwendbar*	√	√
Bandbreite und Traffic	-	*nicht anwendbar*	√	√
Zertifikatsverwaltung	-	*nicht anwendbar*	√	√
Überwachung für mehrere Hersteller	-	*nicht anwendbar*	√	√
Plattform und Lernfunktion für Intelligente Überwachung	-	*nicht anwendbar*	√	√
BACKUP UND WIEDERHERSTELLUNG				
Automatisches Backup	√	*nicht anwendbar*	√	√
Backup-Wiederherstellung	√	*nicht anwendbar*	√	√
Speicherung der Konfigurationshistorie	-	*nicht anwendbar*	√	√
Export von Gerätekonfigurationen	-	*nicht anwendbar*	√	√
SICHERHEIT UND COMPLIANCE				
ISO 27001 – Informationssicherheit	√	*nicht anwendbar*	√	√
ISO 9001 – Qualitätsmanagement	√	*nicht anwendbar*	√	√
NEN 7510 – Informationssicherheit Gesundheitswesen	√	*nicht anwendbar*	√	√
ISAE 3402 Type 2 – Outsourcing-Standard	√	*nicht anwendbar*	√	√
PATCH- UND VERSIONSVERWALTUNG				
Sicherheitsupdates (4)	√	*nicht anwendbar*	√	√
Funktionsupdates (4)	√	*nicht anwendbar*	√	√
SUPPORT				
Geschäftszeiten, 8–18 Uhr	√	*nicht anwendbar*	√	√
Prio-1-Support rund um die Uhr	O	*nicht anwendbar*	O	O

BERICHTERSTATTUNG				
Vorfallsübersicht & Kennzahlen – pro Monat (über Portal)	√	*nicht anwendbar*	√	√
Änderungsübersicht & Kennzahlen – pro Monat (über Portal)	√	*nicht anwendbar*	√	√
Trendanalyse und Empfehlungen – pro Quartal	-	*nicht anwendbar*	√	√

1 Hardware und Software müssen die Funktion unterstützen

2 Die Hardware muss remote erreichbar sein

3 Austausch gegen zusätzliche Kosten

4 Hardware-Supportvertrag erforderlich

6 Anlage 2: Systemanforderungen und -voraussetzungen

6.1 MANAGEMENT-SERVER-ÜBERWACHUNGSSOFTWARE

Beschreibung	Anforderung
Betriebssystem	Windows 7 und höher oder Windows 2012 und höher
(v)CPU	Mindestens 1 vCPU
Arbeitsspeicher	Mindestens 2 GB
Speicher	Mindestens 8 GB
Internetverbindung	Mindestens 5 Mbit/s
Firewall-Konnektivität	Verbindung internes Netzwerk

6.2 FIREWALL-REGELVERWALTUNGSSERVER ZUM INTERNET

URLs	Ports/Konfiguration
*.amazonaws.com	80 & 443
*.security.ubuntu.com	80
*.google.com	80 & 443
DNS	8.8.8.8:53 & 8.8.4.4:53
NTP – Richtlinie erforderlich	pool.ntp.org:123

6.3 FIREWALL-REGELVERWALTUNGSSERVER – INTERNES NETZWERK

Protokolle	Ports
HTTP	80 & 8080
HTTPS	443 & 8443
DNS	53
NTP	123
BGP (Border Gateway Protocol)	179
FTP (File Transfer Protocol)	21, 115, 10021
Java	9010
OSPF (Open Shortest Path First)	89
RADIUS (Remote Authentication Dial-In User Service)	1812
SMTP (Simple Mail Transfer Protocol)	25
SNMP (Simple Network Management Protocol)	161
SSH (Secure Shell)	22
Syslog	514, 54059
TCP Health Check	12345
TFTP (Trivial File Transfer Protocol)	69, 10069
Telnet	23
UPnP (Universal Plug and Play)	1900
mDNS (Multicast DNS)	5353