Forcepoint

Datenblatt

NGFW Security Management Center

Zentrale Verwaltung für maximale Transparenz im Netzwerk

Die wichtigsten Vorteile

- Zentrale Verwaltung von bis zu 6.000 physischen oder virtuellen Forcepoint NGFWs in verteilten Umgebungen über eine einzige Oberfläche
- Flexibilität und Skalierbarkeit für den Einsatz in großen Unternehmensnetzwerken
- Hochverfügbarkeitsoption für hohe Anforderungen an die Betriebszeit
- Intelligente Richtlinien und effiziente Workflow-Automatisierung sorgen für eine schnelle und präzise Bereitstellung und Wartung von Forcepoint NGFWs
- Berücksichtigung des Benutzer- und Endpunktkontextes mit Transparenz im gesamten Netzwerk, vom Rechenzentrum und Edge bis hin zu Zweigstellen und Cloud
- Mehrere Bereitstellungsoptionen als Software oder Appliances stehen zur Auswahl

Durch die überragende Flexibilität, Skalierbarkeit und Benutzerfreundlichkeit erleichtert Forcepoint Security Management Center (SMC) die Verwaltung dynamischer Netzwerksicherheitsumgebungen und unterstützt ambitionierte Unternehmenswachstumspläne. Dank der intelligenten Richtlinien können Geschäftsprozesse in natürlicher Sprache formuliert werden, während die optimierten Arbeitsabläufe die täglichen Verwaltungsaufgaben rationalisieren und so für hohe Effizienz und niedrige Gesamtbetriebskosten (TCO) sorgen.

SMC bietet umfassende Transparenz im gesamten Unternehmensnetzwerk. Für interaktive Untersuchungen sowie detaillierte Berichte ruft SMC Daten zur Ereignisverwaltung und Statusüberwachung von Forcepoint NGFWs, Endpunkten und Geräten von Drittanbietern ab. Darüber hinaus kann Forcepoint SMC NGFW-Protokolldaten von mehreren geografisch verteilten Forcepoint NGFW-Protokollservern abrufen, um konsolidierte Berichte zu erstellen und gleichzeitig die Datenhoheit zu wahren.

Hochverfügbarkeit

Die Unternehmen von heute können sich keine Unterbrechungen leisten und benötigen rund um die Uhr Zugriff auf kritische Ressourcen. Mit der Hochverfügbarkeitsoption von Forcepoint SMC erhalten Unternehmen kontinuierlichen Zugriff auf Protokollressourcen, um eine zuverlässige Analyse und Reaktion auf Vorfälle zu gewährleisten.

Sicherheitsmanagement-Client

Über den Management-Client können Administratoren unabhängig von ihrem geografischen Standort sicher auf Forcepoint SMC zugreifen. Der Client verfügt über eine leistungsstarke Benutzeroberfläche für Konfiguration, Überwachung, Protokollierung, Alarme, Berichte sowie Updates und Upgrades von Forcepoint Next Generation Firewalls. Mit Forcepoint SMC erhalten Administratoren einen umfassenden Überblick über das Netzwerk und profitieren von einer kontextbasierten Detailsuche für eine schnelle und effektive Verwaltung Ihrer gesamten Sicherheitsumgebung.

VERWALTUNGSSERVER	
Anzahl der verwalteten Geräte	Lizenziert: 1 bis 6.000 Knoten mit einem Verwaltungsserver
Anzahl der Administratoren	Unbegrenzt
Anzahl der Elemente	Unbegrenzt
Anzahl der Richtlinien	Unbegrenzt
Anzahl der Protokollserver	Unbegrenzt
Anzahl der Webportal-Server	Unbegrenzt
Administratorauthentifizierung	Lokale Datenbank, RADIUS. TACACS+, Client-Zertifikat und Microsoft Active Directory (LDAP)
Geräteverbindungen	TLS-verschlüsselt
PROTOKOLLSERVER	
Anzahl der unterstützten Geräte	Unbegrenzt
Protokolldatensätze pro Sekunde	Leistungsstarkes Protokollierungssystem, das bis zu 500.000 Datensätze pro Sekunde empfangen kann
Geräteverbindungen	TLS 1.2-Verschlüsselung und Authentifizierung mit X.509v3-Schlüsseln und -Zertifikaten
Protokollspeichergröße	Unbegrenzt
Anzahl der Protokollweiterleitungen je Protokollserver	Unbegrenzt
ALLGEMEIN	
Management-Client	Auf HTML5 basierende UI
SMC-Programmierschnittstelle (SMC API)	Dokumentierte API für eine einfache Integration von Drittanbieterprodukten und -diensten unter Verwendung der REST-Architektur, in der Daten im XML- oder JSON-Format vorliegen können
Mehrere Administratoren	Gleichzeitige Änderungen durch mehrere Administratoren sind möglich; kritische Elemente wie Richtlinien sind für die Bearbeitung gesperrt
Dashboards mit Startbildschirm	Dashboards mit anpassbarem Startbildschirm für NGFWs, VPNs, Benutzer und andere Elemente
Überwachung des Nutzerverhaltens	Neben den vom Nutzerverhalten abhängigen Korrelationen und Prüfungen werden Statusinformationen zur Endpunktsicherheit und Endpunkt-Anwendungsstatistiken bereitgestellt.

Hochverfügbarkeit	Bis zu vier Standby-Verwaltungsserver
Upgrades	Automatisches Herunterladen von Upgrades und dynamischen Update-Paketen
Backups	Integriertes Backup-Tool zum Sichern des gesamten Systems, einschließlich der Konfiguration aller Next Generation Firewalls
Navigation	Intuitive, Browser-ähnliche Navigation mit Suchverlauf, Registerkarten und Lesezeichen
Spotlight-Suchwerkzeuge	Effiziente Tools für die Suche nach Elementen und Referenzen mit kontextsensitiven Sofortaktionen
Schnellfilterfunktion	Komfortables Filtern mit automatischer Worterkennung in Elementlisten, Tabellen und Richtlinienzellen
Unterstützung von Mehrfachauswahl	Durchführen von Aktionen und Übernehmen von Änderungen für Hunderte von Elementen gleichzeitig
Tools zur Systembereinigung	Mit diesen Tools kann der Administrator auf einfache Weise herausfinden, welche Elemente und Regeln nicht verwendet werden.
VERWALTUNG	
Eskalation von Warnungen	Ermöglicht dem Administrator, Warnmeldungen des Systems per E-Mail, SMS, SNMP-Trap und benutzerdefinierten Skripten weiterzuleiten
Grenzwerte für Warnungen	Einfache Grenzwerte für Warnungen in Übersichtsstatistiken
Prüfprotokolle	Alle Änderungen am System werden in Prüfprotokollen aufgezeichnet.
Systemberichte	Bestands- und Compliance-Prüfberichte über die Konten und Aktivitäten von Administratoren
Zero-Touch-Installation	Cloud-basierte (oder USB-Stick-basierte) Installation mit Richtlinienübertragung zu Beginn
Automatisierte Aufgaben	Automatisierte Aufgaben für Protokolldatenverwaltung, Archivierung und Aufbewahrung, Backups, Upgrades und Richtlinienaktualisierung
Verwaltete Domänen	Ermöglichen das Aufteilen der Umgebung in einzelne Konfigurationsdomänen
Import/Export	Export und Import von XML- und CSV-Dateien jederzeit anstatt nur zwischen Installationen
Remote-Upgrades	Ausfallsicheres Remote-Upgrade verwalteter NGFWs mit einem Mausklick
Rollenbasierte Zugriffskontrolle für Administratoren	Definition und Kombination von benutzerdefinierten Rollen zusätzlich zu den vordefinierten Rollen (z. B. Eigentümer, Beobachter, Anwender, Bearbeiter, Superuser), um Berechtigungen flexibel und präzise zu steuern
Lizenzverwaltung	Automatische Online-Lizenzaktualisierung und Statusberichte zum Wartungsvertrag
Zertifikatverwaltung	Konsolidierte Ansicht aller Zertifikate und Berechtigungsnachweise
Tools zur Fehlerbehebung	Umfangreiche Ferndiagnosefunktionen: integriertes Tool zur Erfassung des Datenverkehrs, Download von Konfigurations-Snapshots der Next Generation Firewall und Ansichten zur Sitzungsüberwachung
Incident Case Management	Integrierte Tools für das gemeinsame Management von Netzwerkvorfällen

RICHTLINIENMANAGEMENT	
Virtuelle NGFW-Engine	Gemeinsame Nutzung desselben Master-Kontextes in mehreren SMC-Verwaltungsdomänen; bis zu 250 virtuelle Kontexte mit jeweils eigenen Richtlinien und Routing-Tabellen
Hierarchische Richtlinienverwaltung	Richtlinienvorlagen, untergeordnete Richtlinien, Aliase und Abschnitte mit Regelkommentaren sorgen für Ordnung und Verständlichkeit der Richtlinie
Anwendungserkennung	→ Beschränkung des Zugriffs auf der Basis von Netzwerk- und/oder Endpunkt-Anwendungen → Beschränkung des Zugriffs von/auf Anwendungen nach Nutzlast → Whitelist/Blacklist nach Anwendungsname und Version von Forcepoint Endpoint Context Agent
Change-Management	Überprüfung und Genehmigung durch einen zweiten Administrator, bevor Änderungen implementiert werden
URL-Filterung	Beschränkung des Zugriffs nach URL-Kategorien
Domänennamen	Dynamische Zugriffsbeschränkung anhand von Domänennamen, die in IP-Adressen übersetzt werden können
Benutzeridentifikation	Abgleichen benutzerdefinierter Regeln über eine transparente Benutzeridentifikation oder die Durchsetzung sicherer Authentifizierungsmethoden
Zonen	Kennzeichnung von physischen Schnittstellen durch Zonen und Referenzierung in den Richtlinien
Standortbasierter Schutz	Beschränkung des Zugriffs nach Land oder geografischer Region
Prüfrichtlinien	Detaillierte Kontrolle für Deep Packet Inspection und einfache Methoden zum Ausschließen von Fehlalarmen
QoS-Richtlinien (Quality of Service)	QoS-klassenbasierte Richtlinienkonfiguration
Richtlinienbasierte Dateifilterung	Definiert, wie Dateien mithilfe von McAfee Global Threat Intelligence File Reputation, Anti-Malware Scan und McAfee Advanced Threat Defense geprüft werden
Netzwerkadressübersetzung (NAT)	→ Standard-NAT → Elementbasierte NAT → NAT-Richtlinien
Tool zur Richtlinienvalidierung	Hilft dem Administrator, Konfigurationsfehler vor der Aktivierung der Richtlinie zu finden
Richtlinien-Momentaufnahmen	Ermöglicht Untersuchung und Vergleich der Konfigurationshistorie der Forcepoint Next Generation Firewall
Richtlinienwiederherstellung	Wiederherstellung einer früheren Richtlinienversion und Übertragung an die Next Generation Firewall
Tool zur Optimierung der Regelanwendung	Zeigt Administratoren, wie oft eine Regel innerhalb eines bestimmten Zeitraums erfüllt wurde
Tool zum Suchen von Regeln	Integriertes Tool zum Suchen von Regeln in Richtlinien
Regelnamen	Möglichkeit, Regelnamen zu erstellen, die in Protokollen, Statistiken und Berichten angezeigt werden
Ausfallsichere Richtlinien-Uploads	Beim Ausfall einer neuen Version stellt das System automatisch die vorherige Richtlinienversion wieder her.

KONFIGURATION	
Routing	Routing-Konfiguration per Drag & Drop für die Firewalls und bestimmte Widgets, um Routen und Standardrouten hinzuzufügen
Dynamisches Routing	Erweiterte OSPF- und BGP-Konfiguration über eine intuitive grafische Benutzeroberfläche
Automatisches Anti-Spoofing	Automatische, routingbasierte Erstellung der Anti-Spoofing-Konfiguration
Site-to-Site-VPNs	→ Richtlinienbasiertes IPsec-VPN → Routenbasiertes IPsec-VPN und -Tunneling (GRE)
Remote-Access-VPNs	→ IPsec-VPN-Client (iOS und Windows) → SSL-VPN-Client (Android, Mac und Windows) → Clientloses SSL-VPN-Portal
Verwaltung per Endpoint Context Agent	Erweiterung der Zugriffskontrolle und Transparenz auf die Anwendungen, die auf Endpunkten ausgeführt werden
Firewall Element Creation Wizard	Erstellen von Hunderten von Firewall-Elementen mithilfe eines Firewall-Erstellungsassistenten
Browserbasierte Benutzerauthentifizierung	Konfigurieren und Anpassen eines einfachen browserbasierten Authentifizierungsdienstes für Benutzer
STATUS, STATISTIKEN UND BERICHTE	
Überwachung des Systemstatus	Echtzeit-Statusinformationen über Netzwerkgeräte und deren Verbindungen
Überwachung des Appliance-Status	Grafische Darstellung des Hardwarestatus von Appliances
Netzwerkdiagramme	Visualisierung von Konfigurationen, Topologien und Verbindungsstatus
Sitzungsüberwachung	Dedizierte Ansichten zum Überwachen von Verbindungen, VPN Security Associations (SAs), authentifizierten Benutzern, aktiven Warnungen und dynamischen sowie statischen Routen
Übersichten	Anpassbare Dashboards mit Benutzer- und Netzwerkstatistiken zur Echtzeitüberwachung
Geolokalisierung	Anzeigen von Länderinformationen für alle IP-Adressen mithilfe von Länder-Flags und Standortstatistiken Erkennen, woher Netzwerkangriffe kommen
Berichte	Anpassen und Programmieren von Berichten, die detaillierte Informationen zu Netzwerkstatistiken liefern
Webportal	Schreibgeschützter Zugriff zur Anzeige von Richtlinien, Protokollen und geplanten Berichten

VERWALTUNG VON HARDWARE ANDERER HERSTELLER	
Geräteüberwachung	Ermöglicht dem Administrator, Statusänderungen hinsichtlich der Verfügbarkeit von Drittanbietergeräten zu überwachen und anzuzeigen
Device Log Injection	Analyse und Empfang von Protokollen im Syslog-Format für Drittanbietergeräte und sofort einsatzbereite Unterstützung für CEF-, LEEF-, CLF- und WELF-Format
NetFlow-/IPFIX-Empfang	Möglichkeit, Daten in den Formaten NetFlow v9 und IPFIX zu empfangen, weiterzuleiten und zu konsolidieren
Gerätestatistiken	Grafische Statistiken und Berichte auf Basis von Protokolldaten von Drittgeräten und SNMP-Zählern (Simple Network Management Protocol)
Anzahl der unterstützten Geräte	200 je Protokollserver
Lizenzierung	Jedes Drittanbietergerät beansprucht 0,2 Lizenzen von der Gesamtzahl der Gerätelizenzen am Verwaltungsserver.
PROTOKOLLE	
Browser	Detaillierte Ansicht für die einzelnen Protokolltypen zusätzlich zur allgemeinen Protokollübersicht für alle Protokolldaten
Drag & Drop-Filterung	Interaktives Filtern von Protokollen durch Ziehen und Ablegen einer beliebigen Protokolldatenzelle im Abfragefenster
Statistiken	Erstellen integrierter protokollbasierter Zähler und On-Demand-Statistiken für Berichterstellung, Überwachung und Warnungen
Visualisierung	Erkennen von Auffälligkeiten im protokollierten Datenverkehr durch filterbare Protokollvisualisierungen
Protokollanalyse	Uneingeschränktes Zusammenstellen großer Mengen von nach beliebigen Spalten gefilterten Protokolldaten
Archivierung	Duplizieren und Archivieren von Protokollen in Verzeichnissen anhand von Protokolldatentyp, Zeit oder Filtern
Backups	Integrierter Backup-Planer für die Konfigurations- und Protokolldaten von Protokollservern
Exporte	Export von CSV-, XML- oder LEEF-Dateien oder Protokollen; Protokolle können auch Snapshot-Berichte sein
Weiterleitung	Echtzeit-Protokollumleitung in Syslog; CEF-, LEEF-, XML-, CSV-, IPFIX-, NetFlow- und McAfee Enterprise Security Manager-Formate; Konfiguration für Filterung, Datentyp und Protokollfeldauswahl verfügbar
Datenkontexte	Kurzbefehle zum Durchsuchen verschiedener Protokolltypen mit kontextbezogenen Spaltenlayouts, die angepasst werden können
Hochverfügbarkeit	Unterstützung bei der Zuweisung von primären und Backup-Protokollservern zu jeder Protokollquelle

Zentrale Verwaltung mehrerer Kundenumgebungen

(853 char) Anbieter von Managed Security Services (MSSPs) müssen die hohen Verwaltungskosten senken, die mit der Verwaltung mehrerer Server in verschiedenen Domänen verbunden sind. Mit der Forcepoint Administrative Domain License können mehrere Kundenumgebungen über einen einzigen Verwaltungsserver gesteuert werden. Die Konfigurationen lassen sich wiederverwenden und domänenübergreifend nutzen, um Änderungen schnell und effizient zu verteilen.

Die einzigartige Architektur der Forcepoint Administrative Domain License-Lösung sorgt für unkomplizierte Unternehmens- und MSSP-Umgebungen und erleichtert deren Handhabung. Die rollenbasierte Zugriffskontrolle (RBAC) ermöglicht eine präzise Definition von Administratorverantwortlichkeiten und Domänenzugriffsbeschränkungen. Domänenbasierte Kunden können über ein sicheres, unkompliziertes Webportal problemlos auf Berichte, Richtlinienkonfigurationen und Protokolle zugreifen.

Zentr Forcepoint Administrative Domain License – Spezifikationen

DOMÄNEN	
Maximale Anzahl	1.000
Anzahl der Administratoren	Unbegrenzt
Anzahl der verwalteten Geräte	6.000
Anzahl der Elemente	Unbegrenzt
FUNKTIONEN	
Getrennte Konfigurationen	Unterteilung verwalteter Umgebungen in verschiedene Verwaltungsdomänen, um sicherzustellen, dass die Netzwerkelemente der Kunden nicht durcheinander geraten
Gemeinsam genutzte Konfigurationen	Gemeinsame Nutzung von einzelnen Elementen, wie z. B. Richtlinienvorlagen, für alle Domänen
Zugriffskontrolle	Gewähren oder Beschränken der Zugriffsrechte des Administrators auf die Konfiguration und Transparenz mithilfe separater Verwaltungsdomänen
Überwachung	Überwachen des Status aller vergebenen Domänen anhand einer Domänenübersicht
Branding	Branding von PDF-Berichten mit benutzerdefinierten Formatvorlagen
Migrations-Tools	Verschieben von Elementen zwischen Domänen mit dem integrierten „Move-to-Tool"
Import/Export	Importieren und Exportieren von Elementen von einer SMC-Installation/-Domäne in die andere
Virtuelle NGFW-Engine	Gemeinsame Nutzung desselben Master-Kontextes über Domänengrenzen hinweg mit bis zu 250 virtuellen Kontexten, die jeweils eigene Richtlinien und Routing-Tabellen haben

Forcepoint

forcepoint.com/de/contact