

LANCOM Security Essentials Option

Netzwerksicherheit aus der Cloud

Die LANCOM Security Essentials Option bietet eine effiziente und zuverlässige Lösung, um Netzwerke vor Bedrohungen wie Ransomware, Phishing, Malware oder Diebstahl von Zugangsdaten zu schützen. Durch den integrierten Content Filter werden unerwünschte und illegale Internetinhalte gezielt blockiert – so bleibt die Integrität des Unternehmens gewahrt und das Haftungsrisiko wird deutlich reduziert. Gleichzeitig schützt das BPjM-Modul der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) Minderjährige zuverlässig vor jugendgefährdenden Inhalten. Die zugrunde liegende Datenbank zur Überprüfung der Webseiteninhalte wird DSGVO-konform in einer vertrauenswürdigen Cloud des europäischen Security-Spezialisten Bitdefender gehostet. Für beste Skalierbarkeit ist die Nutzung der Option nicht auf eine bestimmte Nutzeranzahl begrenzt – ideal für wachsende Netzwerke.

- Kategorienbasierte Filterregeln für Webinhalte (Content Filter)
- Zeit- und profilbasierte Konfiguration
- Umfangreiche Nutzungsstatistiken
- Kategoriebasierte Overrides für Webseiten einstellbar
- Unlimitierte Nutzeranzahl
- Sperrung jugendgefährdender Inhalte durch die Webseiten-Liste der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ)
- Einfaches Software-Upgrade für LANCOM SD-WAN Gateways, SD-WAN Central Site Gateways und WLAN-Controller

LANCOM Security Essentials Option

Das Sicherheits-Upgrade für geschäftliche Netzwerke

Mit der LANCOM Security Essentials Option bleibt die Bandbreite des Netzwerks vollständig dem geschäftlichen Betrieb vorbehalten. Webseiten mit Spyware, Phishing, Viren und anderen Bedrohungen werden durch eine leistungsstarke, datenbankgestützte Webfilter-Technologie sicher blockiert. Hierbei erfolgt die Online-Prüfung der angeforderten Webseiteninhalte durch einen externen Bewertungsserver des europäischen Security-Spezialisten Bitdefender. Der Administrator kann frei festlegen, welche thematischen Kategorien gesperrt oder zugelassen werden. Vier vorgefertigte Sicherheitsprofile erleichtern die schnelle und effiziente Implementierung.

Flexible Content Filter-Regeln und individuelle Anpassung

Die LANCOM Security Essentials Option ermöglicht eine feingranulare Steuerung des Internetzugriffs. Kategorienbasierte Filterregeln können für verschiedene Inhaltsarten wie kriminelle, pornografische oder gewalttätige Webseiten definiert werden. Die Regeln sind individuell konfigurierbar und lassen sich durch die Override-Funktion gezielt überschreiben.

Umfassender Schutz vor jugendgefährdenden Inhalten

Das BPjM-Modul der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) sorgt dafür, dass jugendgefährdende Medien gesperrt werden. Dies erfolgt über eine offizielle Webseitenliste der BzKJ, die kontinuierlich aktualisiert und erweitert wird. Dies stellt eine maximale Sicherheit für Minderjährige in Schulen, Freizeiteinrichtungen oder Zuhause sicher.

Individuelle zeit- und profilbasierte Konfiguration

Mit der LANCOM Security Essentials Option lassen sich Internetzugriffsrechte individuell steuern. So können beispielsweise während der Mittagspause bestimmte Inhalte freigeschaltet werden, die während der Kernarbeitszeit gesperrt sind. Ebenso können nutzerabhängige Profile eingerichtet werden, sodass geschäftlich relevante Webseiten selektiv freigegeben werden.

Umfassende Statistiken für volle Kontrolle

Die LANCOM Security Essentials Option bietet detaillierte Statistiken zur Internetnutzung mit Auswertungen nach Kategorien. So lassen sich z. B. Top-10-Listen der blockierten und freigegebenen Webseitenzugriffe für einen einstellbaren Zeitraum erstellen. Die Statistiken werden dabei stets anonymisiert, um Datenschutzrichtlinien einzuhalten.

Flexible Override-Funktion

Bei berechtigtem Bedarf ermöglicht der Override-Button die temporäre Freigabe blockierter Webseiten ohne erneute Konfigurationsanpassung. Die Overrides können kategoriebasiert aktiviert und via E-Mail, SYSLOG oder SNMP überwacht werden, um eine kontrollierte Nutzung sicherzustellen.

LANCOM Security Essentials Option

Security Essentials

Cloud-basierte Security-Engine	Weltweit verteilte und hochverfügbare Bitdefender-Server zur Echtzeit-Abfrage von URL-Klassifizierungen. Datenbank mit über 200 Millionen URLs und 45 Millionen Domains in über 70 Inhaltskategorien. Täglich Analyse von über 1 Milliarde Webanfragen, mehr als 50 Millionen Blockierungen. Automatisierte Kategorisierung durch heuristische Inhaltsklassifikation, Textanalyse, Erkennung von NSFW-Inhalten durch Hautfarbenerkennung in Bildern, Struktur- und Linkanalyse, Bewertung von URL-Reputation basierend auf Telemetriedaten von über 500 Millionen Endpunkten, Honeypots und E-Mail-Fallen. Malware-Erkennung durch Analyse von Webinhalten, Downloads und eingebetteten Objekten. Reaktionszeit unter 100 Millisekunden.
URL-Prüfung*	Datenbankbasierte Online-Prüfung von Webseiten (HTTP/HTTPS). HTTPS-Webseiten werden durch die Entnahme von angesteuerten DNS-Namen aus HTTPS-Serverzertifikaten oder durch "Reverse DNS lookup" der IP-Adresse geprüft und ggfs. blockiert.
Kategorien/Kategorie-Profile*	Definition von Filterregeln pro Profil durch Zusammenstellen von Kategorie-Profilen aus 72 Kategorien, z.B. zur Einschränkung der Internetnutzung auf geschäftliche Anwendungen (Unterbinden privater Nutzung) oder Schutz vor jugendgefährdenden oder gefährlichen Inhalten wie z.B. Malware-Seiten. Übersichtliche Auswahl durch Zusammenstellung thematisch ähnlicher Kategorien zu Gruppen. Inhalte pro Kategorie erlauben, blockieren oder für Override freigeben
Override**	Für Kategorien kann ein Override vergeben werden, der es Anwendern fallweise erlaubt, eigentlich gesperrte Seiten durch manuelle Bestätigung zu laden. Der Override kann zeitlich beschränkt für die Kategorie, die Domäne oder eine Kombination aus beidem ausgesprochen werden. Möglichkeit zur Benachrichtigung eines Administrators im Fall von Overrides
Black-/Whitelist	Manuell konfigurierbare Listen zum expliziten Erlauben (Whitelist) oder Verbieten (Blacklist) von Webseiten pro Profil, unabhängig von der Bewertung durch den Ratingserver. Platzhalter (Wildcards) zur Definition von Gruppen von Seiten oder Filtern von Unterseiten
Profile	Zusammenfassen von Zeitrahmen, Black-/Whitelists und Kategorie-Profilen zu getrennt aktivierbaren Profilen für Filter Aktionen. Werksseitig aktiviertes Default-Profil mit Standard-Einstellungen zum Blocken von pornografischen, kriminellen, extremistischen Inhalten sowie anonymen Proxies, Drogen, SPAM und Malware
Zeitrahmen	Flexible Definition von Zeitrahmen, um Profile zur Filterung in Abhängigkeit von Tageszeiten oder Wochentagen zu definieren, z. B. für Lockerung während Pausenzeiten für privates Surfen
Flexibel anwendbare Firewall-Aktion	Anwendung durch Content Filter Aktionen mit Auswahl des gewünschten Profils in der Firewall. Firewall-Regeln ermöglichen die flexible Anwendung eigener Profile für verschiedene Clients, Netze oder Verbindungen zu bestimmten Servern
Individuelle Rückmeldungen (bei blockiert, Fehler, Override)	Antwortseiten des Content Filters für blockierte Seiten, Fehler und Override können individuell gestaltet und durch Variablen mit aktuellen Informationen zu Kategorie, URL und Kategorisierung des Ratingservers versehen werden. Sprachabhängige Definition von Antwortseiten, je nach vom Anwender ausgewählter Anzeigesprache des Webbrowsers
Umleitung zu externen Webseiten	Alternativ zur Anzeige der geräteinternen Antwortseiten für blockierte Seiten, Fehler oder Override können auch Seiten von externen Webservern aufgerufen werden (Redirect)
Lizenzmanagement	Automatische Benachrichtigung vor Ablauf der Lizenz per E-Mail, LANmonitor, SYSLOG und SNMP-Trap. Aktivierung der nächsten Lizenz-Verlängerung zu beliebigem Zeitpunkt vor dem Ablauf der aktuellen Lizenz (Start des neuen Lizenzzeitraumes passend zum Ablauf der aktuellen Lizenz)

LANCOM Security Essentials Option

Security Essentials

Statistiken	Anzeige der Anzahl der geprüften und gesperrten Webseiten je Kategorie in LANmonitor. Logging aller Content-Filter-Events in LANmonitor; tägliches, wöchentliches oder monatliches Anlegen einer Protokolldatei. Hitliste der meist aufgerufenen Seiten und Ratingergebnisse. Auswertung der Verbindungseigenschaften, minimalen, maximalen und durchschnittlichen Antwortzeiten des Ratingservers
Alarmierungen	Benachrichtigung bei Content-Filterung einstellbar via E-Mail, SNMP, SYSLOG sowie LANmonitor
Assistent für Standard-Konfigurationen	Assistent zur Einrichtung des Content Filters für typische Anwendungsszenarien in wenigen Schritten, inklusive Erzeugung der nötigen Firewall-Regeln mit entsprechender Aktion
Voraussetzung	Voraussetzung für die Nutzung der Security Essentials Option ist LCOS 10.92 oder höher
*) Hinweis	Die Kategorisierung erfolgt durch Bitdefender. Die jederzeitige Richtigkeit der Kategorisierungen können weder Bitdefender noch LANCOM garantieren.
**) Hinweis	Die Override-Funktionalität steht nur für HTTP-Seiten zur Verfügung.

Artikelnummern

62168	LANCOM Security Essentials B Option 1 Jahr (für LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller LANCOM WLC-60)
62169	LANCOM Security Essentials B Option 3 Jahre (für LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller LANCOM WLC-60)
62170	LANCOM Security Essentials B Option 5 Jahre (für LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller LANCOM WLC-60)
62171	LANCOM Security Essentials C Option 1 Jahr (für LANCOM SD-WAN Gateways der 1900-Serie und LANCOM 2100EF)
62172	LANCOM Security Essentials C Option 3 Jahre (für LANCOM SD-WAN Gateways der 1900-Serie und LANCOM 2100EF)
62173	LANCOM Security Essentials C Option 5 Jahre (für LANCOM SD-WAN Gateways der 1900-Serie und LANCOM 2100EF)
62174	LANCOM Security Essentials D Option 1 Jahr (für LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller LANCOM WLC-2000)
62175	LANCOM Security Essentials D Option 3 Jahre (für LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller LANCOM WLC-2000)
62176	LANCOM Security Essentials D Option 5 Jahre (für LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller LANCOM WLC-2000)