



Cisco ASA mit FirePOWER Services

Erweiterte Sicherheit für kleine und mittelständische Organisationen sowie Großunternehmen mit verteilten Standorten

Unternehmen aller Größenordnungen sind von kostspieligen Angriffen immer größeren Ausmaßes betroffen, die eine Gefahr für Kundendaten, Unternehmensressourcen und geistiges Eigentum darstellen. Die **2013 Information Security Breaches Survey**, in Auftrag gegeben von der britischen Regierung, ergab, dass 87 % aller kleinen Unternehmen 2012 durch Sicherheitsbedrohungen beeinträchtigt wurden. Großunternehmen veranlassen zur Verbesserung der Sicherheit ihre Partner, wie z. B. Rechtsanwaltskanzleien, dazu, ihren Bedrohungsschutz zu optimieren, damit diese nicht selbst zur Bedrohung für das Unternehmen werden können.

Vorteile

- **Überragender Bedrohungsschutz** mit der branchenführenden Sicherheitstechnologie der Cisco® Next-Generation Firewalls
- **Angemessene Größe und attraktiver Preis** für Budgets kleiner und mittelständischer Unternehmen, einschließlich geringer Gesamtbetriebskosten
- **Vereinfachtes integriertes Management oder optional zentrales Management** für Installationen auf mehreren Geräten

Sowohl kleine als auch mittelständische Organisationen und Großunternehmen mit verteilten Standorten haben hohe Anforderungen an den Schutz vor Bedrohungen. Bislang konnten Unified Threat Management(UTM)-Produkte und NGFWs anderer Anbieter diesen Anforderungen nicht gerecht werden. Im Gegensatz zu diesen veralteten Ansätzen bieten die NGFWs von Cisco Advanced Malware Protection (AMP) und Next-Generation IPS (NGIPS). Die neuesten Ergänzungen zur NGFW-Familie der Cisco® ASA mit FirePOWER™ Services wurde für kleine und mittelständische Unternehmen (KMUs) und Anwendungen in Zweigstellen entwickelt. Sie bieten integrierten Schutz vor Sicherheitsbedrohungen und vereinfachtes Sicherheitsmanagement bei geringen Beschaffungs- und Betriebskosten.

Die Lösung ist als Desktop-Variante (5506-X) und im 1 HE Rackmontage-Formfaktor (5508-X, 5516-X) erhältlich. Die Varianten des Desktop-Modells sind mit einem integrierten Wireless Access Point (5506W-X) verfügbar, um die Vernetzung in KMUs zu vereinfachen.

Es wurde auch eine besonders robuste Appliance (5506H-X) für industrielle Kontrollsysteme und geschäftskritische Infrastrukturanwendungen entwickelt. Sie umfasst einen erweiterten Betriebstemperaturbereich und ist als Desktop- oder DIN-Schienen-¹, Rack- oder Wandmontage-Modell erhältlich.

Überragender Wert, besonderer Schutz vor Sicherheitsrisiken und flexible Managementoptionen.

Die Cisco Next-Generation Firewall-Lösungen bieten überragenden Wert und branchenführenden Schutz vor Sicherheitsrisiken, inklusive Firewall, Anwendungskontrolle, NGIPS, URL-Filterung, Cisco Advanced Malware Protection (AMP) und VPN. Mit maximaler Transparenz und Kontrolle sowie automatischer Priorisierung der Sicherheitsrisiken können Fehlalarme, die ansonsten zu viel Arbeitszeit in Anspruch nehmen würden, effizient verwaltet werden.

¹ DIN-Schiene: Der Begriff leitet sich von den vom Deutschen Institut für Normung (DIN) veröffentlichten ursprünglichen Spezifikationen her, die seither als europäische (EN) und internationale (ISO) Standards übernommen wurden.

Nachweise

- Die Cisco ASA wurde 2014 in der weltweit vierteljährlich stattfindenden Security Appliance Track-Studie von IDC als am häufigsten eingesetzte Firewall der Welt genannt.
- Der Cisco AnyConnect VPN Client ist mit mehr als 100 Millionen Bereitstellungen der führende VPN-Client der Welt und vollständig kompatibel mit Cisco ASA mit FirePOWER Services.
- Die Cisco ASA mit FirePOWER Services nutzt die täglichen Cisco Security Intelligence Feeds, damit Sicherheitsrisiken rechtzeitig erkannt werden können.

Merkmale und Funktionen

Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X und 5516-X mit FirePOWER Services

Benutzer-/Node-Support	Standardmäßig unbegrenzt
Desktop-Version (5506-X, 5506W-X)	20,12 x 22,66 x 4,39 cm
Rackmount-Version (5508-X, 5516-X)	43,69 x 28,67 x 4,40 cm
Version für starke Beanspruchung (5506H-X)	22,99 x 22,99 x 6,91 cm
Integrierte E/A-Ports	8 x 1GE

VPN

VPN-Peers	50-300
Mobilitätsunterstützung	AnyConnect 4.x; native Apple iOS- und Android-Clients

Durchsatz

Max. Stateful Firewall	750 Mbit/s-1,8 Gbit/s
Max. AVC	250-850 Mbit/s
Max. AVC und NGIPS	125-600 Mbit/s
Hohe Verfügbarkeit	Ja: Aktiver/Standby-Modus* Aktiv/Aktiv (nur 5508-X und 5516-X)

NGFW-Funktionen

AVC	Bei SmartNet inbegriffen
Unterstützte Anwendungen	Mehr als 3000
URL-Filterung	Abonnement
Kategorien; Gesamt	80+; 280+ Millionen
NGIPS	Abonnement
Signaturen	6000+
AMP – Bedrohungsschutz	Abonnement

Management

Integriertes On-box-Management	Standardmäßig inbegriffen
Zentrales Management	Optionale Lizenz

* Erfordert Security Plus-Lizenz

Weitere technische Daten entnehmen Sie bitte dem Datenblatt zur ASA mit FirePOWER Services.

Die Cisco Security-Lösungen beschleunigen zudem die Reaktion auf Vorfälle. So berichten Kunden häufig, dass die Behebung des Problems von mehreren Wochen auf wenige Stunden verkürzt wurde.

Zwar wurden diese NGFW-Modelle von Cisco eigens für kleine und mittelständische Unternehmen (KMU) entwickelt, sie bieten jedoch dieselben überragenden Technologien zum Schutz vor Sicherheitsrisiken wie andere Next-Generation Firewalls der Cisco ASA 5500-X-Serie, darunter Cisco ASA 5525-X und 5585-X. Beide erreichten in der NSS Labs **Next-Generation Firewall Security Value Map 2014** das höchste Wirksamkeits-Rating hinsichtlich ihrer Sicherheit. Die NGFWs von Cisco umfassen integriertes Management für Single-Instance-Bereitstellungen und unterstützen wo erforderlich zentrales Management mit dem Cisco FireSIGHT Management System.

Standardmerkmale und -funktionen der Cisco ASA mit FirePOWER Services

- Cisco Application Visibility and Control (AVC):** Cisco AVC unterstützt über 3000 Kontrollen auf Anwendungsebene und Risikobasis. Beispielsweise können Sie bei beliebigen Social-Media-Anwendungen einen Schreibschutz festlegen, um die Einhaltung von Vorschriften der US-amerikanischen Financial Industry Regulatory Authority (FINRA) oder des Health Insurance Portability and Accountability Act (HIPAA) zu ermöglichen und Nutzungsrichtlinien durchzusetzen.
- Führende Netzwerk-Firewall sowie Support für Site-to-Site- und Remote-Access-VPN:** Im Vergleich mit der Konkurrenz genießen die Firewall und das VPN von Cisco weltweit am meisten Vertrauen und werden am häufigsten eingesetzt. Der optionale Cisco AnyConnect® VPN-Client lässt sich auf einfache Weise mit den Cisco ASA mit FirePOWER Services integrieren. Cisco AnyConnect 4.0 bietet ein präzises, stets verfügbares VPN auf Anwendungsebene. Darüber hinaus unterstützt die Cisco ASA mobile und native Android- und iOS-VPN-Clients von Cisco AnyConnect.

Abonnementoptionen für Cisco FirePOWER Services

- NGIPS** bietet marktführende kontextbezogene Erkennung, umfassende Transparenz, Kontrolle für Benutzer, Geräte, Anwendungen und Inhalte sowie branchenführende Prävention von Sicherheitsrisiken.
- AMP** verfügt über branchenführende Funktionen, mit denen Malware und Sicherheitsrisiken, die von anderen Sicherheitsebenen übersehen werden, erkannt, verstanden, gestoppt und behoben werden können.
- Die reputationsbasierte URL-Filterung** blockiert risikoreiche Web-Adressen. Spam, URL-basierte Viren, Phishing-Angriffe und Spyware können Benutzer auf schädliche URLs weiterleiten. Cisco analysiert URLs sorgfältig und ordnet ihr einen Reputationswert zu, sodass Benutzer Web-Adressen mit hohem Risiko meiden können.

Nächste Schritte

Wenden Sie sich an einen Cisco Partner in Ihrer Region:

[Einen Cisco Partner finden.](#)