



**WatchGuard
FireboxCloud / FireboxV –
Auslagerung von Diensten in die Cloud**

Agenda

- Darstellung FireboxV
 - Lizenzmodelle
 - Unterschiede Firebox und FireboxV
 - Besonderheiten bei der FireboxV

- Darstellung Firebox Cloud (AWS & Azure)
 - Überblick und Lizenzmodelle
 - Unterschied zur Firebox

- Beispiele von Einsatz-Szenarien

FireboxV

- FireboxV ist die Version von virtuelle Firebox für VMware und Hyper-V
 - FireboxV für VMware unterstützt:
 - VMware ESXi 6.0, 6.5 & 6.7
 - FireboxV für Microsoft Hyper-V unterstützt:
 - Windows Server 2008 R2 und Hyper-V Server 2008 R2
 - Windows Server 2012 R2 und Hyper-V Server 2012 R2
 - Windows Server 2016 und Hyper-V Server 2016
 - Windows Server 2019 und Hyper-V Server 2019

- Unterstützt alle Firewall Funktionen und Services

FireboxV

- Vier FireboxV Modelle
 - Small, Medium, Large, Extra Large
- FireboxV Ressourcen Anforderungen
 - 5 GB Storage
 - CPU und Speicher Anforderung unterscheiden sich per Model

FireboxV Model	vCPUs (Maximum)	Memory (Recommended)
Small	2	1024 MB
Medium	4	2048 MB
Large	8	4096 MB
Extra Large	16	4096 MB

Unterschiede Firebox und FireboxV

- Die FireboxV bietet den Benutzer wie die Firebox einen vollständigen Schutz vor Bedrohungen jeglicher Art.
- Die FireboxV unterstützt alle UTM Features.
- Einige Funktionen werden aber nicht von der FireboxV unterstützt.
 - Aktiv/Aktiv FireCluster im VMware ESXi Umgebung
 - Bridge Mode (Netzwerk Konfiguration)
 - Hardware Diagnose Befehle über die CLI
 - Automatische Speicherung eines Support Snapshot auf ein USB-Laufwerk
 - Automatische Wiederherstellung eines Backups von einem USB-Laufwerk

Unterschiede Firebox und FieboxV

- Für einige Funktionen muß der „promiscuous mode“ in der Netzwerkeinstellung des Hypervisor aktiviert werden.
 - Für folgendes Funktionen ist das der Fall:
 - Drop-in mode network configuration
 - Network bridge
 - Mobile VPN with SSL, with the **Bridged VPN Traffic** setting
- Microsoft Hyper-V unterstützt kein „promiscuous mode“ und kann somit folglich die oben genannten Punkte auch nicht unterstützen.
- Des Weiteren unterstütz Microsoft Hyper-V auch keinen FireCluster
!

Installation – Was ist anders !

- Die Installation verläuft wie bei physikalischen Firebox Appliance.
- Einige Dinge sind aber zu beachten:
 - Die FireboxV hat zwei (2) Interfaces, EXTERNAL und TRUSTED
 - Das Interface TRUSTED hat die IP Adresse 10.0.1.1 zugewiesen.
 - Das Interface EXTERNAL wird eine IP Adresse über DHCP zugewiesen.
 - Das Interface TRUSTED hat kein DHCP Server aktiviert.
 - Beide Interfaces erlauben Management Verbindungen per HTTPs und WSM.
 - Das Konto **admin** hat die default passphrase **readwrite**.
 - Wenn die Serial Nummer der FireboxV mit 000000000 endet, ist die FireboxV noch nicht aktiviert.



Firebox Cloud



Überblick und Lizenzmodelle

Was ist die “Firebox Cloud”?

- Eine virtuelle Firebox für Amazon Web Services (AWS) und Microsoft Azure

- Funktionen und Vorteile
 - Schützt eine AWS Virtual Private Cloud (VPC) oder ein MS Azure Netzwerk (Vnet) vor Angriffen wie Botnets, Cross-Site-Scripting, SQL-Injection-Versuche und anderen Angriffs-Vektoren
 - Angepasste Web UI für AWS & MS Azure
 - Ermöglicht eine sichere VPN Verbindung
 - Monitoring und Reporting mit Cloud Visibility oder Dimension
 - Unterschiedliche Optionen zum Kauf einer Lizenz

Firebox Cloud Kauf Optionen

- Zwei Optionen für den Erwerb von Lizenzen bestehen in den Marketplace der Anbieter
 - Bring Your Own License (BYOL)
 - Erwerb einer Firebox Cloud Lizenz von einem WatchGuard Reseller
 - Pay As You Go
 - Erwerb einer Firebox Cloud-Instanz im AWS-Marktplatz
- Beide Optionen stellen (fast) die gleichen Firewall-Funktionalitäten und Sicherheitsdienste bereit.

Lizenz Option- BYOL

- Erwerb einer Firebox Cloud Lizenz von einem WatchGuard Reseller
 - Das Modell definiert die Anzahl der vCPUs, die es verwenden kann

Firebox Cloud Model	Maximum AWS vCPUs
Small	2
Medium	4
Large	8
Extra Large	16

- Die Firebox Cloud Instanz sollte die maximale Anzahl von vCPUs, die Ihr Modell unterstützt, aufweisen.
- Aktivieren der Lizenz im WatchGuard-Portal und aktualisiere der Firebox Cloud Lizenz (in der WebUI)

Lizenz Option – Pay As You Go

- Abrechnung der Nutzung erfolgt über die Dienstleister (AWS oder MS Azure)
- Es ist keine Aktivierung oder Feature Key erforderlich
- Zu der monatlichen Lizenzkosten kommen noch weitere Kosten für die Nutzung der Cloud (Traffic, Speicher, IP Adresse, ...)



Unterschied zur Firebox



Unterstützte Subscription Services

- Firebox Cloud unterstützt folgende Subscription Services:
 - Access Portal (requires Fireware v12.1 or higher)
 - Application Control
 - APT Blocker
 - Botnet Detection
 - Data Loss Prevention
 - DNSWatch (supported with a BYOL license only)
 - Gateway AntiVirus / Intelligent AntiVirus
 - Geolocation

Unterstützte Subscription Services

- Firebox Cloud unterstützt folgende Subscription Services:
 - Intrusion Prevention Service (IPS)
 - Reputation Enabled Defense
 - spamBlocker and Quarantine Server (requires Fireware v12.2 or higher)
 - Threat Detection and Response (TDR Host Sensor licenses included with a BYOL license only)
 - WatchGuard Cloud Visibility (supported with a BYOL license only)
 - WebBlocker

Network Interface Konfiguration

- Firebox Cloud unterstützt bis zu 8 Netzwerk-Schnittstellen

- Alle Schnittstellen verwenden DHCP, um eine IP-Adresse anzufordern
 - Es gibt keine Schnittstelleneinstellungen in der Web UI

- Die Verwaltung der Schnittstellen Einstellung (Ip Adresse, Ip Adressbereich, usw.) erfolgt innerhalb der Verwaltung des Cloud-Dienstes.
 - Die FireboxCloud setzt auf die Netzwerk Struktur des Provides auf !

Funktion Unterschied — Netzwerk

■ *Nicht unterstützte Netzwerkfunktionen*

- Drop-in mode and Bridge mode
- DHCP server and DHCP relay (all interfaces are DHCP clients)
- PPPoE
- IPv6
- Multi-WAN (includes sticky connections and policy-based routing)
- ARP entries
- Link Aggregation
- VLANs
- FireCluster
- Bridge interfaces

Funktion Unterschied – Richtlinien und Dienste

- Folgende Richtlinien und Dienste werden nicht unterstützt:
 - Explicit-proxy and Proxy Auto-Configuration (PAC) files
 - Quotas
 - (DNSWatch)
 - Network Discovery
 - Mobile Security
- Authentifizierung Funktionen werden nicht unterstützt:
 - Hotspot
- Weitere nicht unterstützte Funktionen sind
 - Gateway Wireless Controller
 - Mobile VPN with SSL Bridge VPN Traffic option

Standardkonfigurationseinstellungen

- Veränderte Standardeinstellungen für Firebox Cloud
 - Alle Schnittstellen verwenden DHCP, um eine primäre IPv4 IP-Adresse zu erhalten
 - Mehr als ein Geräteadministrator kann gleichzeitig angemeldet sein
 - Über jede Schnittstelle kann eine Verbindung mit Fireware Web UI hergestellt und verwaltet werden
 - Die Standardrichtlinien erlauben Managementverbindungen und Pings zur Firebox Cloud, erlauben aber keinen ausgehenden Datenverkehr aus den privaten Subnetzen über die Firebox Cloud
 - Der Setup Wizard richtet nicht die lizenzierten Subscription Services ein

Beispiele von Einsatz-Szenarien



Scenarien

- Virtuelle Systeme eignen sich in vieler Hinsicht Dienste einer physikalischen Firebox auszulagern.
- Je nach System (FireboxV oder FireboxCloud) unterscheiden sich manche Ansätze.
- Z.B. kann man keine FireboxCloud in einem internen Netzwerk für die Separierung von Netzen verwenden.

Scenarien

- Gemeinsame Scenarien können sein
 - VPN Endpunkt für Client Verbindungen
 - VPN Endpunkt für Server Verbindungen
 - Schutz von internen Ressourcen mit Hilfe von
 - Access Portal (Reverse Proxy)
 - Host Header Redirection (Veröffentlichung von Servern nach Extern)

- Alle diese Ansätze haben einen gemeinsamen Ansatz
 - Entlastung der physikalischen Firebox

Beispiel

- Ein Kunde schickt seine Mitarbeiter in das Home Office. Seine WatchGuard Firebox hat 50 Lizenzen für Mobile User VPN per SSL. Der Kunde hat aber 89 Mitarbeiter im Home Office.

- Die Lösung könnte sein:
 1. Er macht ein Upgrade auf eine Firebox M370

 2. Er lagert das VPN Gateway zu einen lokalen ISP aus (FireboxV) oder in die Cloud (Firebox Cloud)
 - Über eine BOVPN zwischen der on-premise Firebox und der virtuellen Instance können die User auf die internen Ressourcen zugreifen.

Beispiel

- Der Kunde hat mehrere Webserver on-premise. Er hat aber nun mehr Anfragen, da sich sein Geschäftsmodell in das Internet verlagert hat. Seine Internet-Leitung kann die benötigte Bandbreite nicht mehr darstellen.

- Die Lösung könnte sein:
 1. Eine zweite Internet Leitung oder eine Erhöhung der Bandbreite
 2. Auslagerung des oder der Webserver in die Cloud (ISP/ Azure/AWS).
 - BOVPN zwischen beiden Instanzen.

WatchGuard Hilfen

- COVID-19 stellt viele Unternehmen vor neuen Herausforderungen.
- Unter folgenden Link finden sie nützliche Informationen zu unseren Produkten und Lizenzen bezogen auf Home Arbeitsplätze.
- WatchGuard Resources to Aid with Remote Worker Security (<https://www.watchguard.com/wgrd-solutions/remote-worker>)
- FireboxV Test Lizenzen wurden auf 120 Tage verlängert (<https://www.watchguard.com/wgrd-blog/watchguards-response-covid-19>)





Vielen Dank!



***NOTHING GETS
PAST RED.***



WatchGuard Training

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved