



Best Practices - FireboxCloud / FireboxV

Agenda

- FireboxV
 - Lizenzmodelle
 - Unterschiede Firebox und FireboxV
 - Installation – Was ist anders !
 - Besonderheiten bei der FireboxV
- Firebox Cloud
 - Überblick und Lizenzmodelle
 - Unterschied zur Firebox
 - Installation und Konfiguration
- Demo Firebox Cloud

Einführung

- Hypervisor Systeme wie Vmware ESXi und Microsoft Hyper-V sind in der heutigen IT Landschaft nicht mehr wegzudenken.
- Diese Systeme müssen wie ihre vergleichbaren, physikalischen Systeme genauso geschützt und überwacht werden.
- WatchGuard bietet seit 2012 die XTMv, nun FireboxV, als virtuelle Systeme für seine Kunden an.

FireboxV

- FireboxV ist die neue Version von virtuelle Firebox für VMware und Hyper-V
 - FireboxV für VMware unterstützt:
 - VMware ESXi 5.5, 6.0, 6.5
 - 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
- Unterstützung aller Fireware 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 Backup von einem USB Laufwerk

Unterschiede Firebox und FieboxV

- Für einige Funktionen müssen, um im Hypervisor zu funktionieren, 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 TUSTED 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 das eine nicht aktivierte FireboxV.

Besonderheiten bei der FireboxV

ESXi

- Empfehlungen für die Ressourcenverteilung

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

- Je nach Version können bis zu 10 Interfaces aktiviert werden (eth0 bis eth9).

Besonderheiten bei der FireboxV

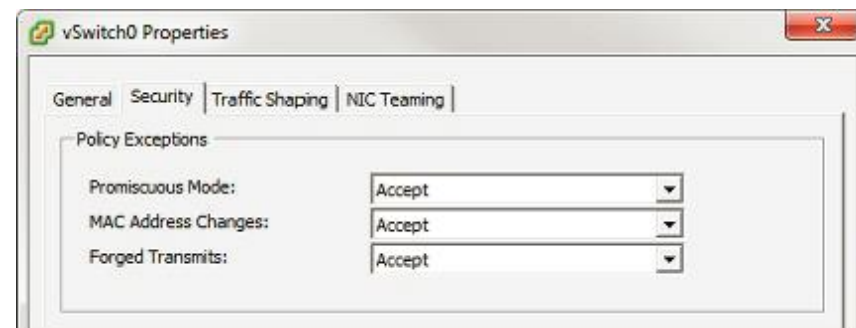
ESXi

- Virtuelle Switch Konfiguration
 - Um mehrere VLAN auf dem ESXi Netzwerkschicht zu verwenden, muß auf dem entsprechenden vSwitch als VLAN ID 4095 (ALL) eingetragen werden.
- Bei Verwendung eines FireCluster muss der vSwitch folgendermaßen konfiguriert werden:

„promiscuous mode“ und

„accept MAC address changes“

aktiviert.



Besonderheiten bei der FireboxV

Hyper-V

- Empfehlung für die Ressourcenverteilung ist entsprechend wie bei ESXi Server.
- Netzwerk Adapter:
 - Hyper-V unterstützt bis zu acht (8) Netzwerkadapter
 - Hyper-V unterstützt bis zu vier (4) „Legacy“ Netzwerkadapter. Diese können aber bei den Betrieb einer FireboxV **NICHT** verwendet werden.

Einsatzszenarien

FireboxV

- Die FireboxV bietet eine vielfältige Möglichkeit.
- Einige Einsatzszenarien sind
 - Network at a Service – Hosting
Der Schutz von Mandaten Daten in gehosteten Umgebungen.
 - Cloud Data Center
Sicherung von Anwendungen im Cloud Umfeld.
 - Segmentierung
Abgrenzung von internen Unternehmensstrukturen. Sicherung von physikalischen oder virtuellen Umgebungen.



Firebox Cloud AWS



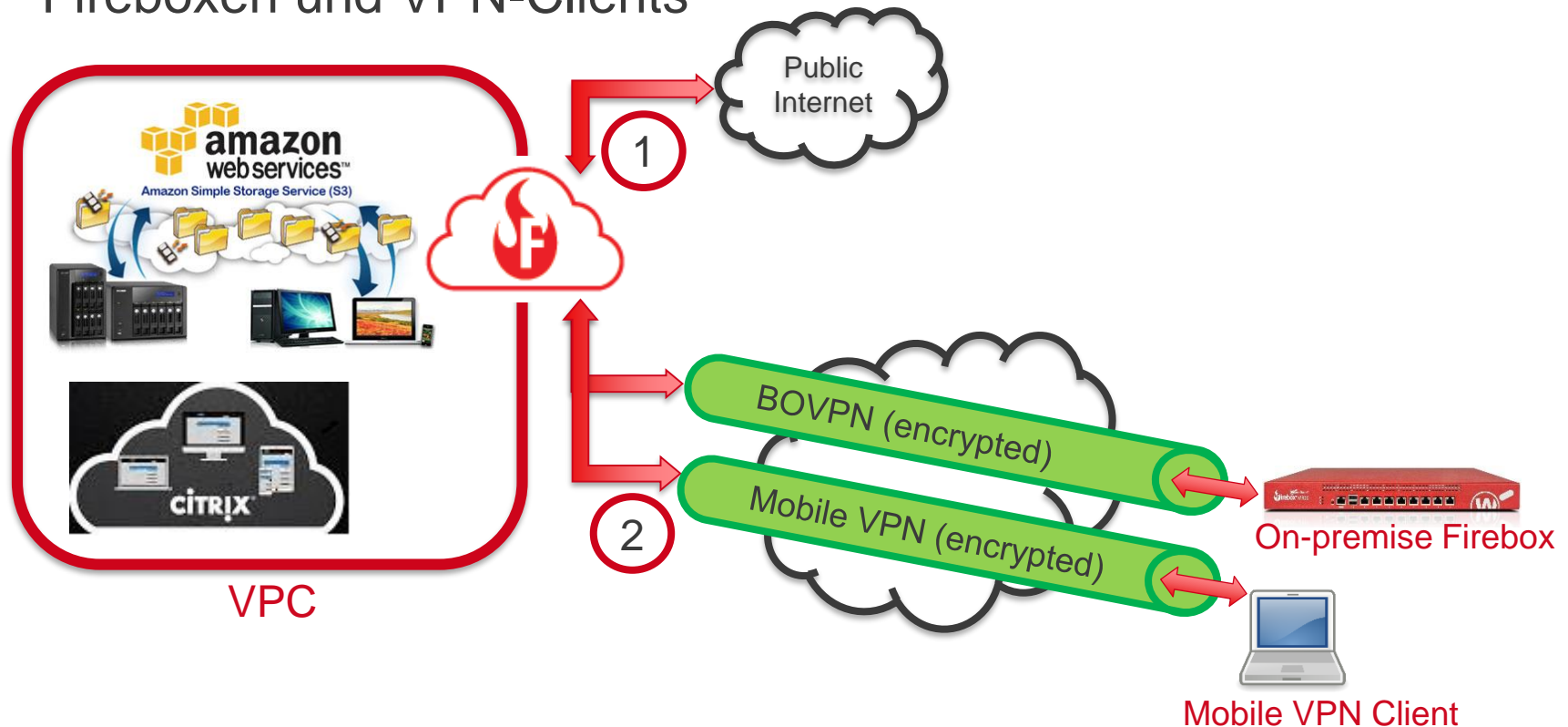
Überblick und Lizenzmodelle

Was ist die “Firebox Cloud”?

- Eine virtuelle Firebox für Amazon Web Services (AWS)
 - Fireware v11.12.1
 - Features und Services, die auf die AWS-Umgebung zugeschnitten sind
- Funktionen und Vorteile
 - Schützt eine AWS Virtual Private Cloud (VPC) vor Angriffen wie Botnets, Cross-Site-Scripting, SQL-Injection-Versuche und anderen Angriffs-Vektoren
 - Angepasste Web UI für AWS
 - Ermöglicht eine sichere VPN Verbindung zum AWS VPC
 - Kompatibel mit Dimension für Monitoring und Reporting
 - Unterschiedliche Optionen zum Kauf einer Lizenz

Primäre Nutzungsfälle

1. Schutz eines Servers / Service unter AWS (Firewall und Security Services)
2. Aufbau einer VPN-Verbindungen zu AWS von WatchGuard Fireboxen und VPN-Clients



Firebox Cloud Kauf Optionen

- Zwei Optionen im AWS Marketplace
 - 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 die gleichen Fireware-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

- Einrichten einer Firebox Cloud Instanz in Amazon EC2, die die maximale Anzahl von vCPUs hat, die Ihr Modell unterstützt
- Aktivieren der Lizenz im WatchGuard-Portal und aktualisiere der Firebox Cloud Lizenz (in der WebUI)

Lizenz Option – Pay As You Go

- Amazon überwacht die Nutzung der Firebox Cloud und erstellt eine Rechnungen basierend auf diesen Daten
- Es ist keine Aktivierung oder Feature Key erforderlich

Unterschied zur Firebox



Administration

- Firewall Web UI ist das primäre Verwaltungs Programm
 - Firewall CLI wird auch unterstützt
- Dimension wird nur für das Monitoring und Erstellung von Reports verwendet
- Für die Verwaltung der Firebox Cloud können nicht eingesetzt werden:
 - WatchGuard Management Server
 - Policy Manager
 - Dimension Command

Unterstützte Subscription Services

- Firebox Cloud unterstützt folgende Subscription Services:
 - Application Control
 - WebBlocker
 - Gateway AV
 - Geolocation
 - Intrusion Prevention Service (IPS)
 - Reputation Enabled Defense
 - Botnet Detection
 - Data Loss Prevention
 - APT Blocker
 - Threat Detection and Response

Network Interface Konfiguration

- Firebox Cloud unterstützt bis zu 8 Netzwerk-Schnittstellen
 - 1 External
 - Bis zu 7 Internal
- Alle Schnittstellen verwenden DHCP, um eine IP-Adresse anzufordern
 - Es gibt keine Schnittstelleneinstellungen in der Web UI
- Unter AWS müssen folgendes eingestellt werden:
 - Konfigurieren der Schnittstellen für die Instanz
 - Zuweisen einer Elastic IP (EIP) Adresse für die Externe Schnittstelle

Funktion Unterschied — Netzwerk

- Nicht unterstützte Netzwerkfunktionen
 - Drop-in Mode und Bridge Mode
 - DHCP Server und DHCP Relay
 - PPPoE
 - IPv6
 - Multi-WAN
 - Static ARP
 - Link Aggregation
 - VLAN Bridge Interface
 - FireCluster
 - Gateway Wireless Controller
 - Mobile VPN mit SSL Bridge VPN Traffic Option

Funktion Unterschied – Richtlinien und Dienste

- Folgende Richtlinien und Dienste werden nicht unterstützt:
 - Explicit-proxy und Proxy Auto-Configuration (PAC) Datei
 - Quotas
 - spamBlocker und Quarantine Server
 - Network Discovery
 - Mobile Security
- Authentifizierung Funktionen werden nicht unterstützt:
 - Hotspot
 - Single Sign-On (SSO)

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



Installation und Konfiguration

AWS Terminology

- Amazon Virtual Private Cloud (VPC)
 - Ein isoliertes, privates, virtuelles Netzwerk in der AWS Cloud
- Elastic Compute Cloud (EC2) Instanz
 - Ein virtueller Server - Firebox Cloud - läuft als EC2-Instanz
- Elastic IP Address (EIP)
 - Eine statische öffentliche IP-Adresse, die Sie einer EC2-Instanzschnittstelle zuordnen - Für die Firebox Cloud wird diese der Eth0 Schnittstelle zugewiesen
- Security Group
 - Eine virtuelle Firewall von AWS, die den eingehenden und ausgehenden Datenverkehr steuert und welche erlaubt, eine EC2-Instanz zu erreichen

Einrichtung - Überblick

- Folgende Punkte sind zu beachten:
 1. Erstellen einer VPC mit öffentlichen und privaten Subnetzen
 2. Beenden der Standard-NAT-Instanz für die VPC
 3. Erstellen einer Firebox Cloud EC2-Instanz in der VPC
 4. Konfigurieren der Netzwerkeinstellungen in AWS für die EC2-Instanz

- Weitere Informationen finden Sie im Firebox Cloud Deployment Guide

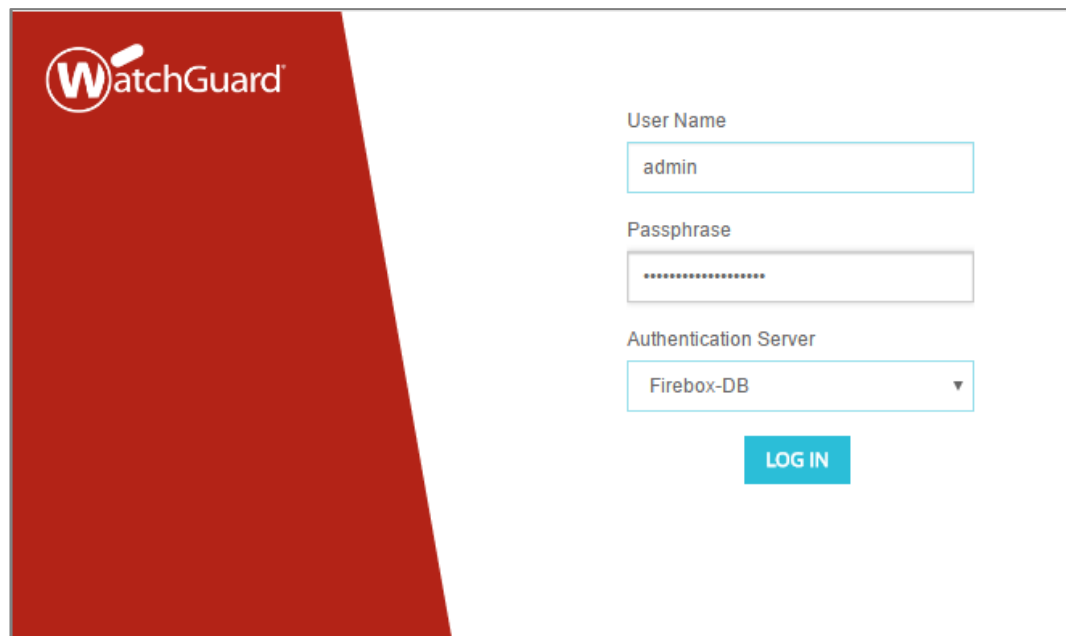
Verbindung zur Firebox Cloud Web UI

- Um sich mit der Web UI zu verbinden, braucht man folgende Informationen:
 - Elastic IP - Adresse, um eine Verbindung zu Fireware Web UI herzustellen
 - Instance ID – Die Standard Passphrase für die Firebox Cloud

The screenshot shows the AWS Management Console interface. The top navigation bar includes 'Services', 'Resource Groups', and user information 'Cindy @ 8409-0693-3262' in 'N. California'. The left sidebar shows navigation options like 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'Instances', 'Spot Requests', 'Reserved Instances', 'Dedicated Hosts', 'IMAGES', 'AMIs', 'Bundle Tasks', and 'ELASTIC BLOCK STORE', 'Volumes'. The main content area displays a table of EC2 instances. One instance is highlighted: 'FB_Cloud_D...' with Instance ID 'i-0767ae8755052d54a', Instance Type 't2.micro', Availability Zone 'us-west-1b', and State 'running'. Below the table, the details for this instance are shown. The 'Instance ID' 'i-0767ae8755052d54a' and the 'Elastic IP: 52.9.26.153' are both highlighted with red boxes. The 'Description' tab is selected, showing details like 'Instance state: running' and 'Instance type: t2.micro'. Other details include 'Public DNS: ec2-52-9-26-153.us-east-1.compute.amazonaws.com', 'Public IP: 52.9.26.153', and 'Elastic IPs: 52.9.26.153*'. The 'Status Checks' and 'Monitoring' tabs are also visible.

Firebox Cloud Setup Wizard

- Bei der ersten Verbindung werden im Firebox Cloud Setup Wizard die Passphrasen für die Administrator- und Statusbenutzerkonten gesetzt.
 - User Name: admin
 - Passphrase: Die Firebox Cloud Instance ID



The screenshot shows the WatchGuard logo in the top left corner. The main content area contains a login form with the following fields:

- User Name:** A text input field containing the text "admin".
- Passphrase:** A text input field filled with dots, representing a masked password.
- Authentication Server:** A dropdown menu with "Firebox-DB" selected and a downward arrow.
- LOG IN:** A blue button with white text.

Firebox Cloud Setup Wizard

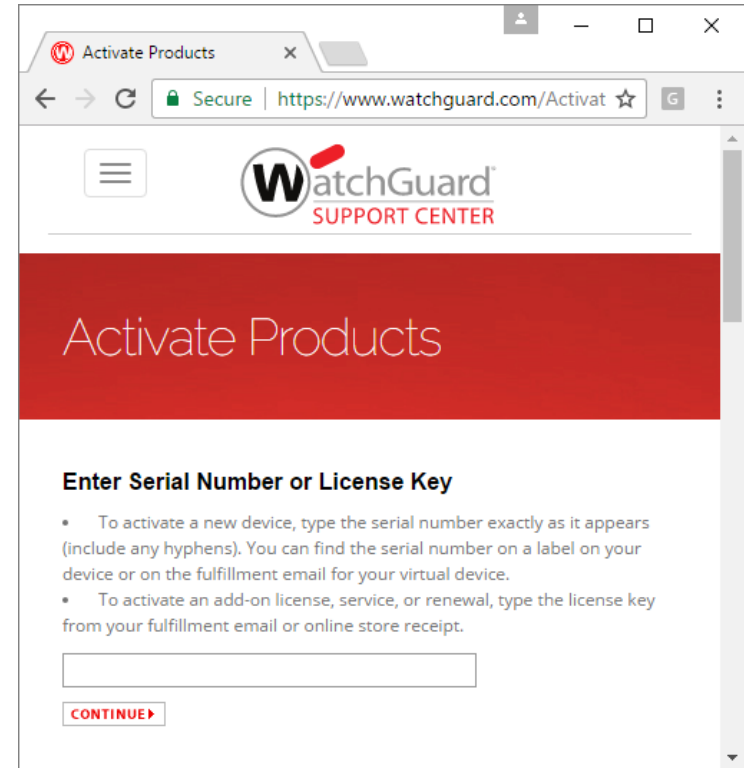
- Akzeptieren der EULA und setzen der Passphrasen

The screenshot shows the WatchGuard Fireware Web UI interface. At the top, there is a red header with the WatchGuard logo and the text "Fireware Web UI". To the right of the header, there is a "User:" label followed by a question mark icon and a user profile icon. The main content area is titled "Create passphrases for your Firebox Cloud". Below the title, there is a section that says "Your Firebox Cloud has two built-in user accounts:". Underneath, it lists two accounts: "admin has read-write privileges." and "status has read-only privileges.". Below this, there is a prompt: "Type the passphrase to use with each account. Each passphrase must contain between 8 and 32 characters.". There are two sets of input fields. The first set is for the "status (read-only)" user, with fields for "User name" (pre-filled with "status (read-only)"), "Passphrase", and "Confirm passphrase". The second set is for the "admin (read-write)" user, with fields for "User name" (pre-filled with "admin (read-write)"), "Passphrase", and "Confirm passphrase". At the bottom right of the form, there are two buttons: "BACK" and "NEXT".

- Nach setzen der Passphrasen wird die Firebox sofort neu gestartet

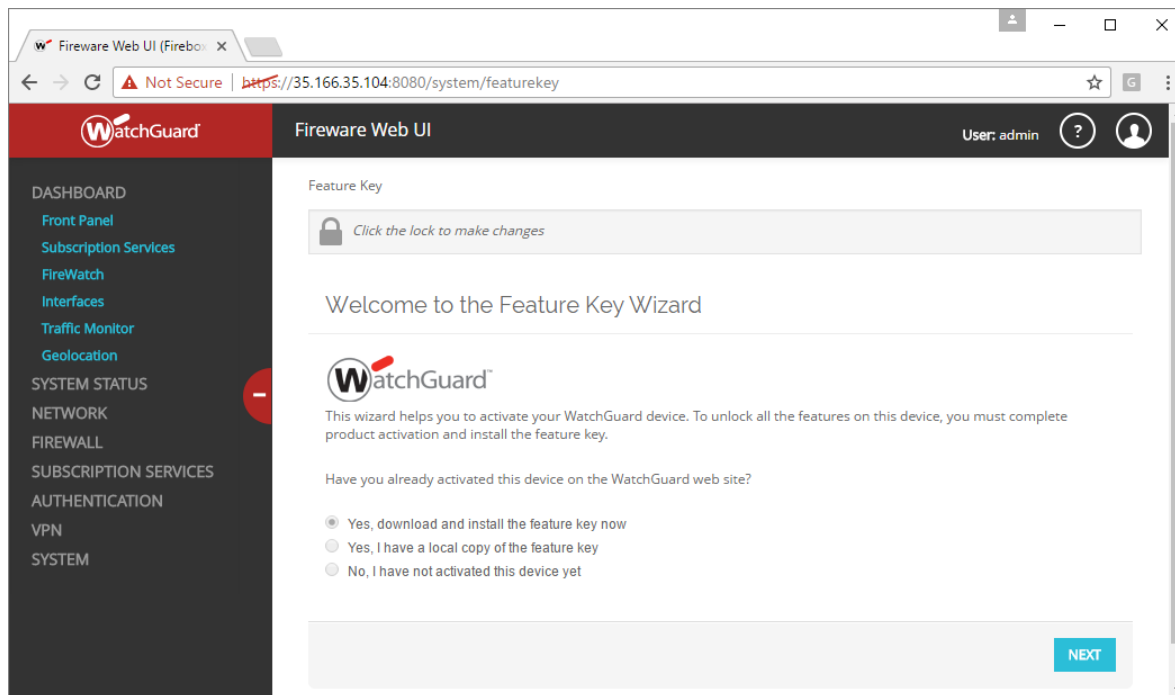
Feature Key hinzufügen (BYOL)

- Beim Kauf einer Firebox Cloud bekommt man eine Seriennummer
- Aktivieren Sie die Seriennummer im WatchGuard Portal, nachdem Sie die Instanz bereitgestellt haben
 - Während der Aktivierung müssen Sie die Firebox Cloud-Instanz-ID angeben
 - Der Aktivierungsprozess erzeugt für diese Instanz eine Feature Key
 - Sie können den Feature Key nur auf eine Firebox Cloud-Instanz mit der angegebenen Instanz-ID anwenden



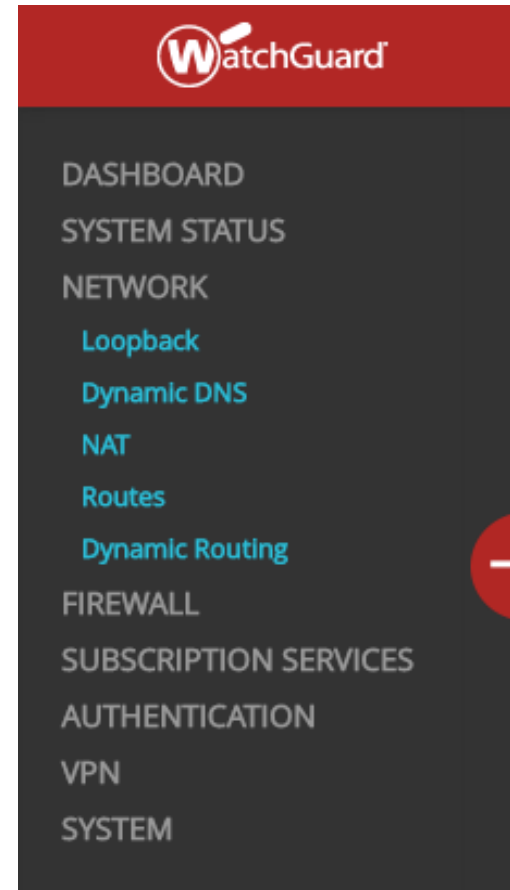
Feature Key hinzufügen (BYOL)

- Der Feature Key Wizard ist der gleiche wie für jede andere Firebox
 - Herunterladen oder einfügen
- Wurde der Feature Key hinzugefügt, startet die Firebox automatisch mit einer neuen Seriennummer



Fireware Web UI für Firebox Cloud

- Fireware Web UI ist sehr ähnlich der Standard Web UI, wurde für die AWS-Umgebung angepasst.
- Funktionen, welche nicht unterstützt werden, wurden ausgeblendet.
- Viele Netzwerkooptionen sind in Fireware Web UI nicht konfigurierbar, da die Netzwerkschnittstellen in der AWS-Konsole konfiguriert werden.



Fireware Web UI für Firebox Cloud

- Das **Front Panel** Dashboard zeigt AWS Instanz Informationen

The screenshot displays the WatchGuard Fireware Web UI Front Panel dashboard. The interface includes a navigation sidebar on the left with categories like DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, and SYSTEM. The main content area is titled 'Front Panel' and features several sections: 'Top Clients', 'Top Destinations', and 'Top Policies', each with a table of active connections. A 'System' information panel on the right provides details about the device, including its name, model, version, and instance information. The instance information is highlighted with a red box, showing the Instance Type as 't2.micro', Instance ID as '04d20fa3335b0907e', and Availability Zone as 'us-west-2c'. A 'REBOOT' button is visible at the bottom of the system panel.

Fireware Web UI (Firebox) x

Not Secure | <https://35.166.35.104:8080/dashboard/#frontpanel>

WatchGuard Fireware Web UI User: admin

Front Panel

Top Clients View all

NAME	RATE	BYTES	HITS
208.146.43.6	12 Kbps	1 KB	1

Top Destinations View all

NAME	RATE	BYTES	HITS
10.0.0.107	12 Kbps	1 KB	1

Top Policies View all

NAME	RATE	BYTES	HITS
WatchGuard W	12 Kbps	1 KB	1

System

Name	Firebox
Model	FireboxCloud-MC
Version	11.12.1.B519746
Instance Type	t2.micro
Instance ID	04d20fa3335b0907e
Availability Zone	us-west-2c
Serial Number	1P120002C001
System Time	23:03 Greenwich
System Date	2017-01-23
Uptime	12 days 00:45
Log Server	Disabled
Threat Detection	Connected
Dimension	Disabled

REBOOT

Fireware Web UI für Firebox Cloud

- Das **Interfaces** Dashboard zeigt Schnittstellenkonfigurationsinformationen für die Firebox Cloud-Instanz

The screenshot shows the WatchGuard Fireware Web UI interface. The left sidebar contains a navigation menu with the following items: DASHBOARD, Front Panel, Subscription Services, FireWatch, Interfaces (highlighted with a red box), Traffic Monitor, Geolocation, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'Interfaces' and features a '20 MINUTES AGO' refresh button. Below the title, there are two tabs: 'Bandwidth' and 'Detail' (highlighted with a red box). The 'Detail' tab displays configuration information for two interfaces:

External (eth0)		Enabled	Yes
		Link Status	Up
Enabled	Yes	Interface ID	eni-2dfec37d
Link Status	Up	Public Hostname	ec2-35-166-35-104.us-west-2.compute.amazonaws.com
Zone	External	Public IPv4	35.166.35.104
IPv4 Address	10.0.0.107/24	Local Hostname	ip-10-0-0-107.us-west-2.compute.internal
Gateway	10.0.0.1	Device Number	0
MAC Address	0A:49:69:5F:67:AB	VPC ID	vpc-40508c27

Trusted (eth1)		Enabled	Yes
		Link Status	Up
Enabled	Yes	Interface ID	eni-edfbc6bd
Link Status	Up	Local Hostname	ip-10-0-1-182.us-west-2.compute.internal
Zone	Trusted	Device Number	1
IPv4 Address	10.0.1.182/24	VPC ID	vpc-40508c27



Live Demo – Firebox Cloud AWS



Vielen Dank!



***NOTHING GETS
PAST RED.***



WatchGuard Training

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved