Best Practices - FireboxCloud / FireboxV

WatchGuard Training

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 FieboxV

- 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 einen 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

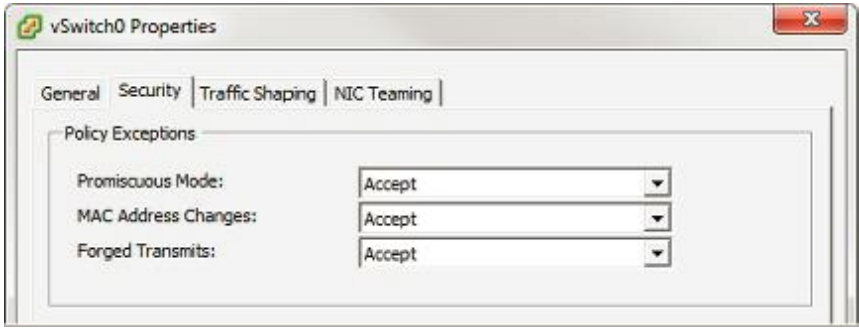
ESXi

- Virtuelle Switch Konfiguration
  - Um mehrere VLAN auf dem ESXi Netzwerkswitch 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

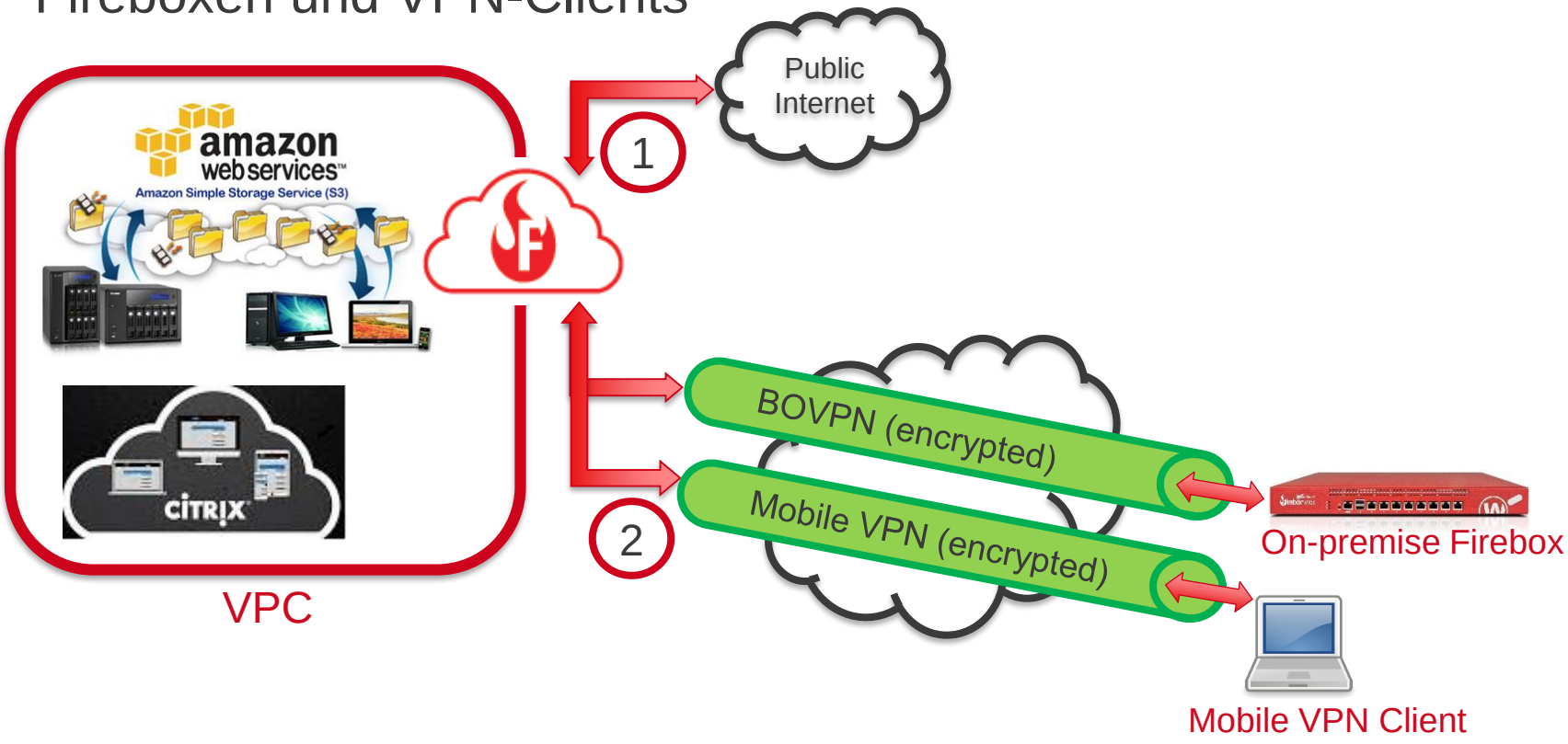
Überblick und Lizenzmodelle

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

- Fireware Web UI ist das primäre Verwaltungs Programm
  - Fireware 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 herstellt 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

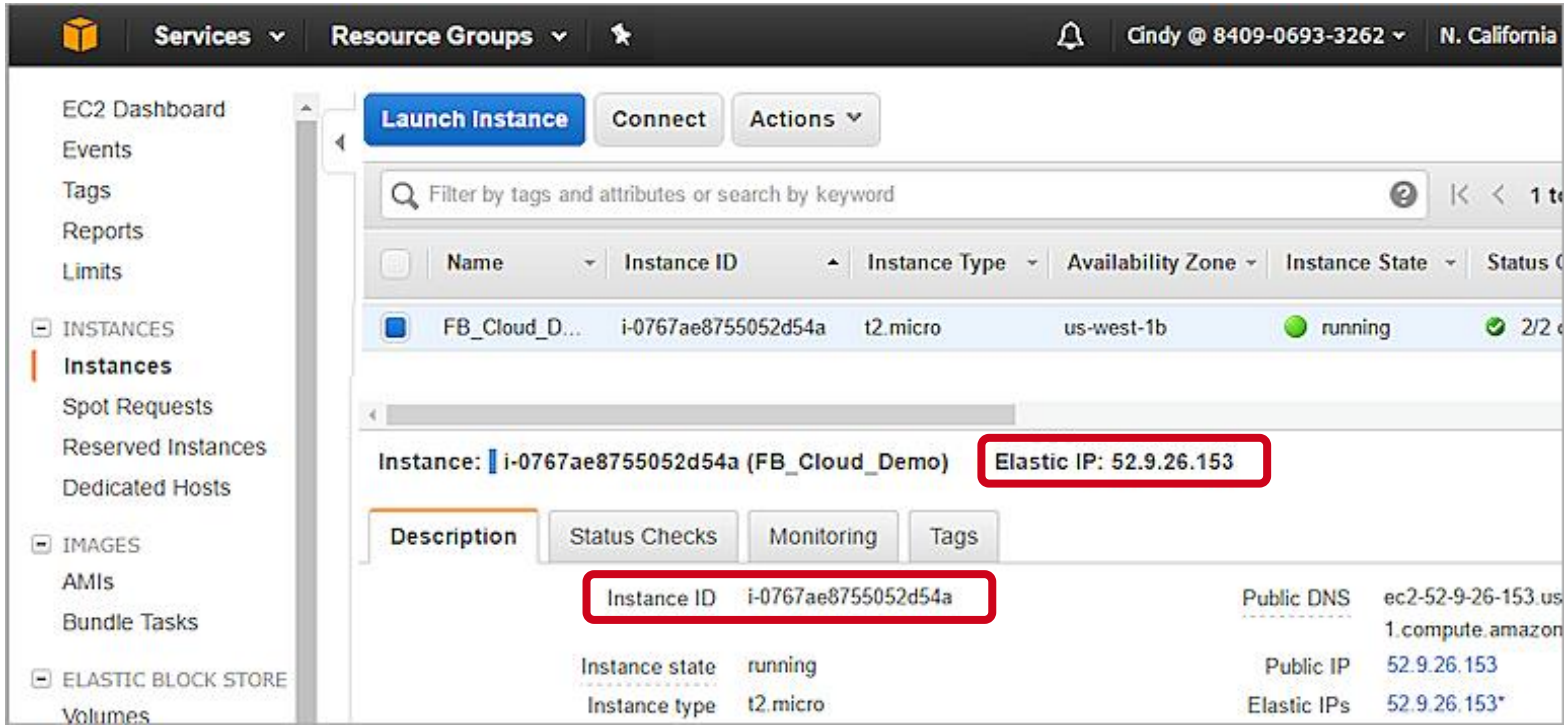
Einrichtung - Überblick

- 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

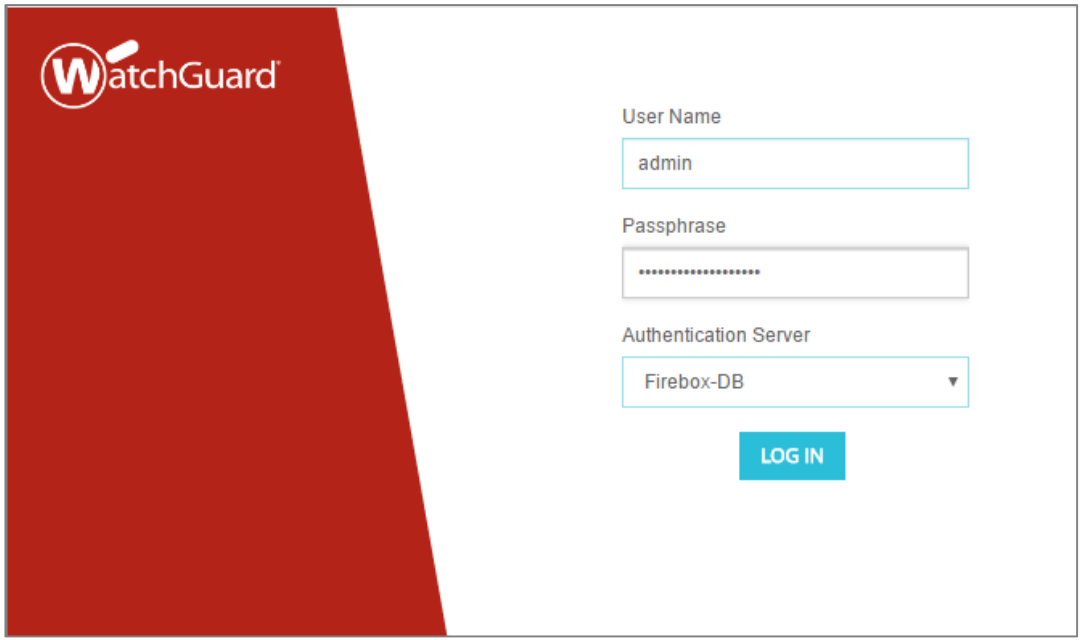
Verbindung zur Firebox Cloud Web UI

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



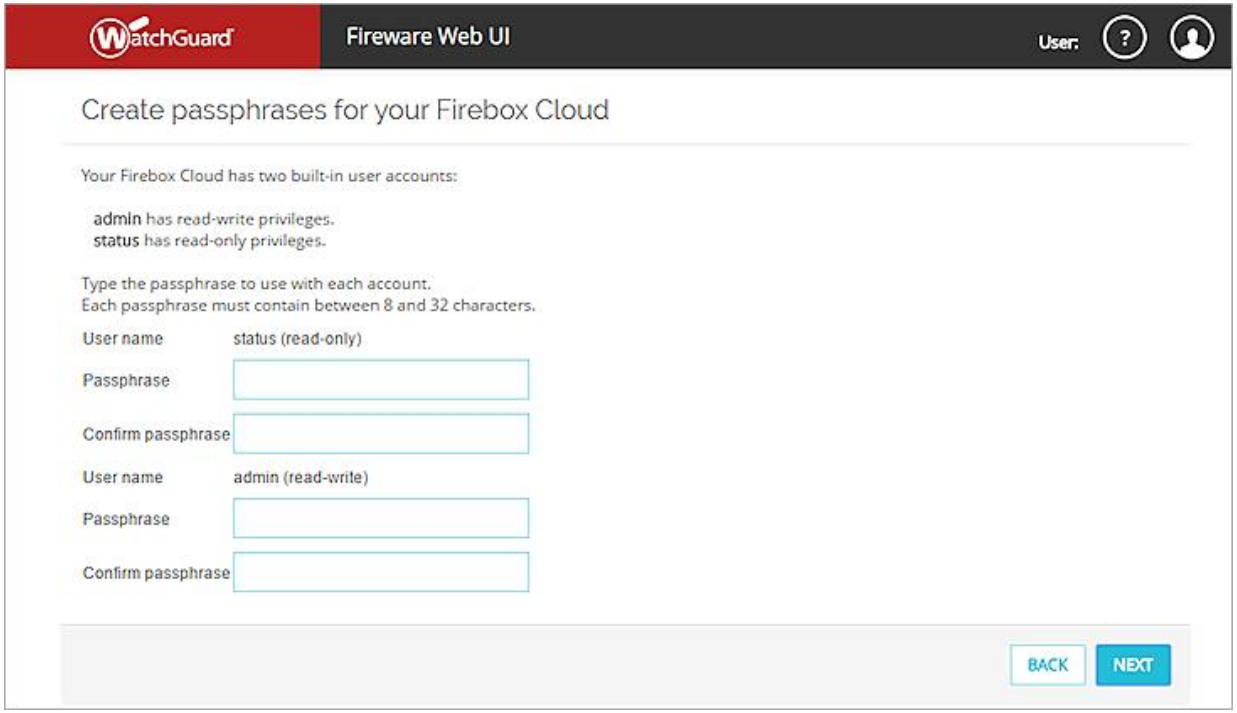
Firebox Cloud Setup Wizard

- 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



Firebox Cloud Setup Wizard

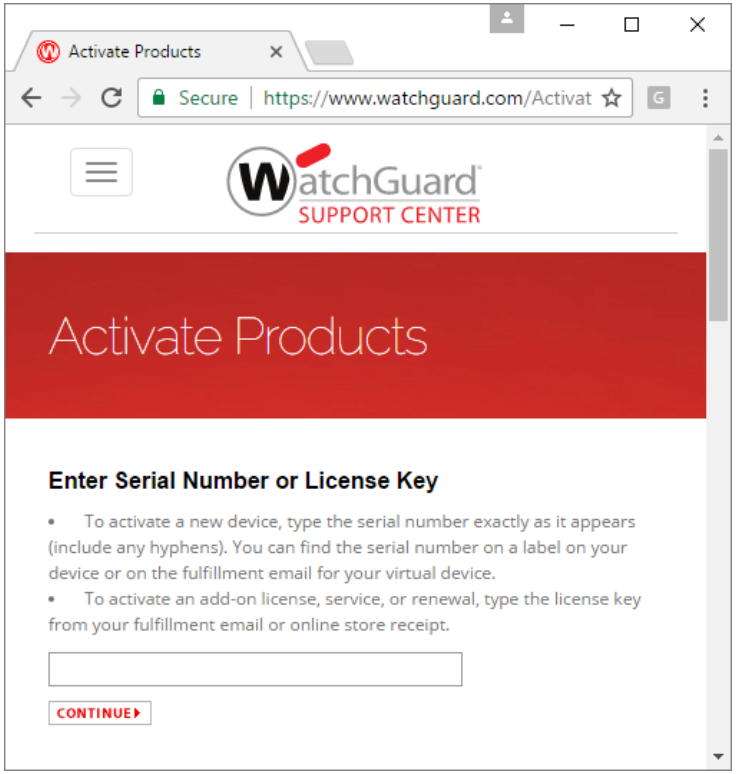
- Akzeptieren der EULA und setzen der Passphrasen



- Nach setzen der Passphrasen wird die Firebox sofort neu gestartet

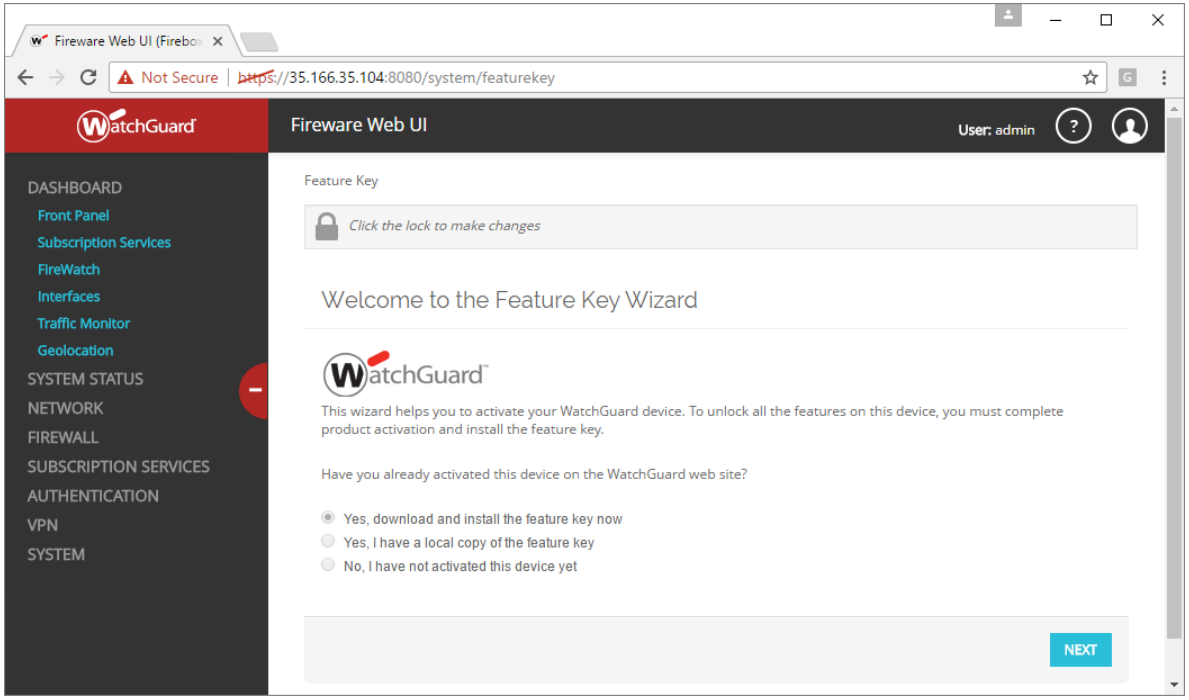
Feature Key hinzufügen (BYOL)

- 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



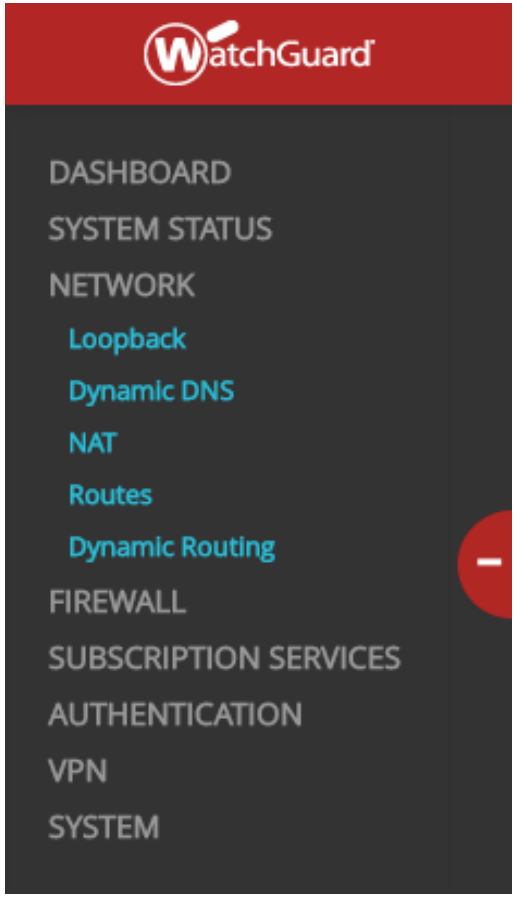
Feature Key hinzufügen (BYOL)

- 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



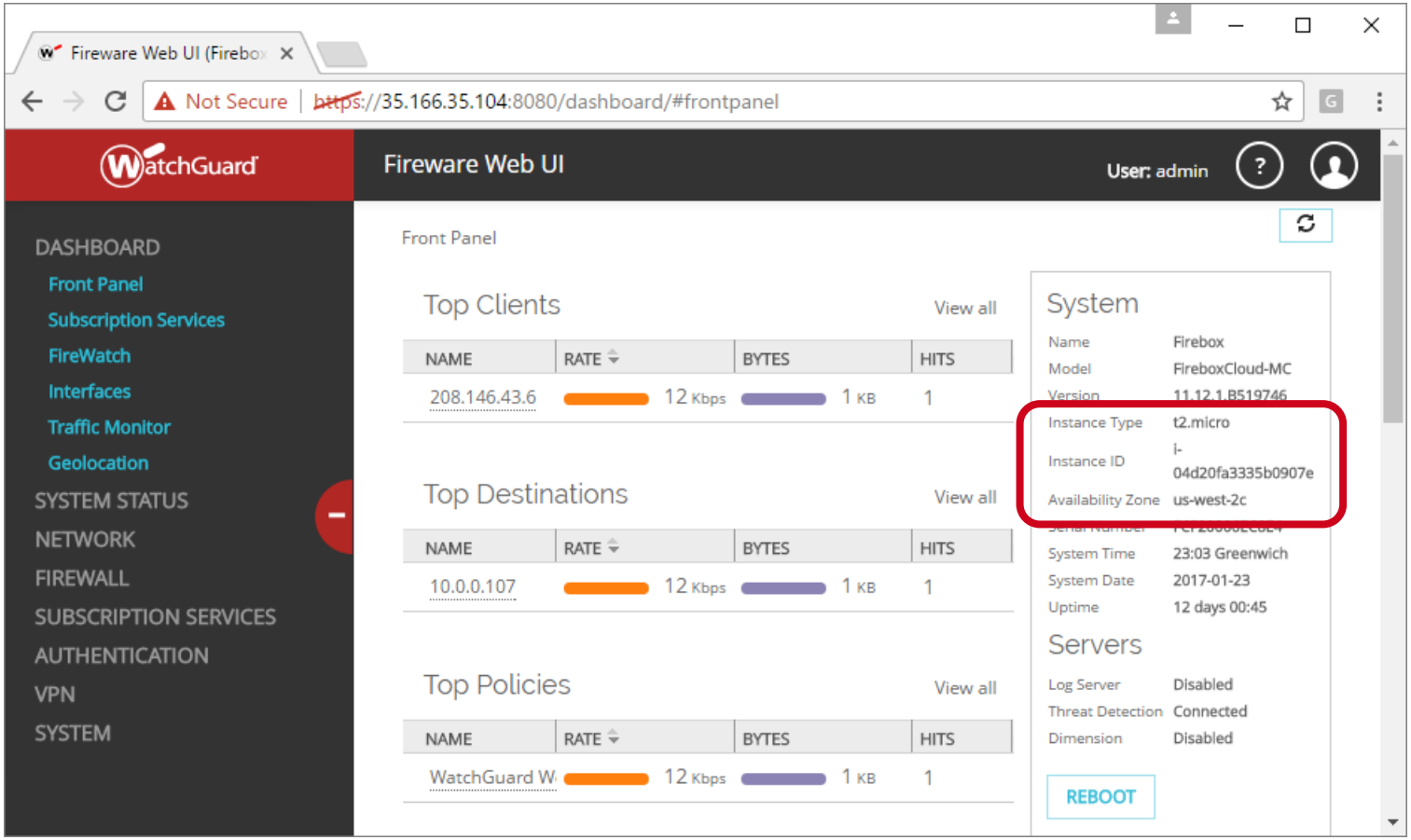
Fireware Web UI für Firebox Cloud

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



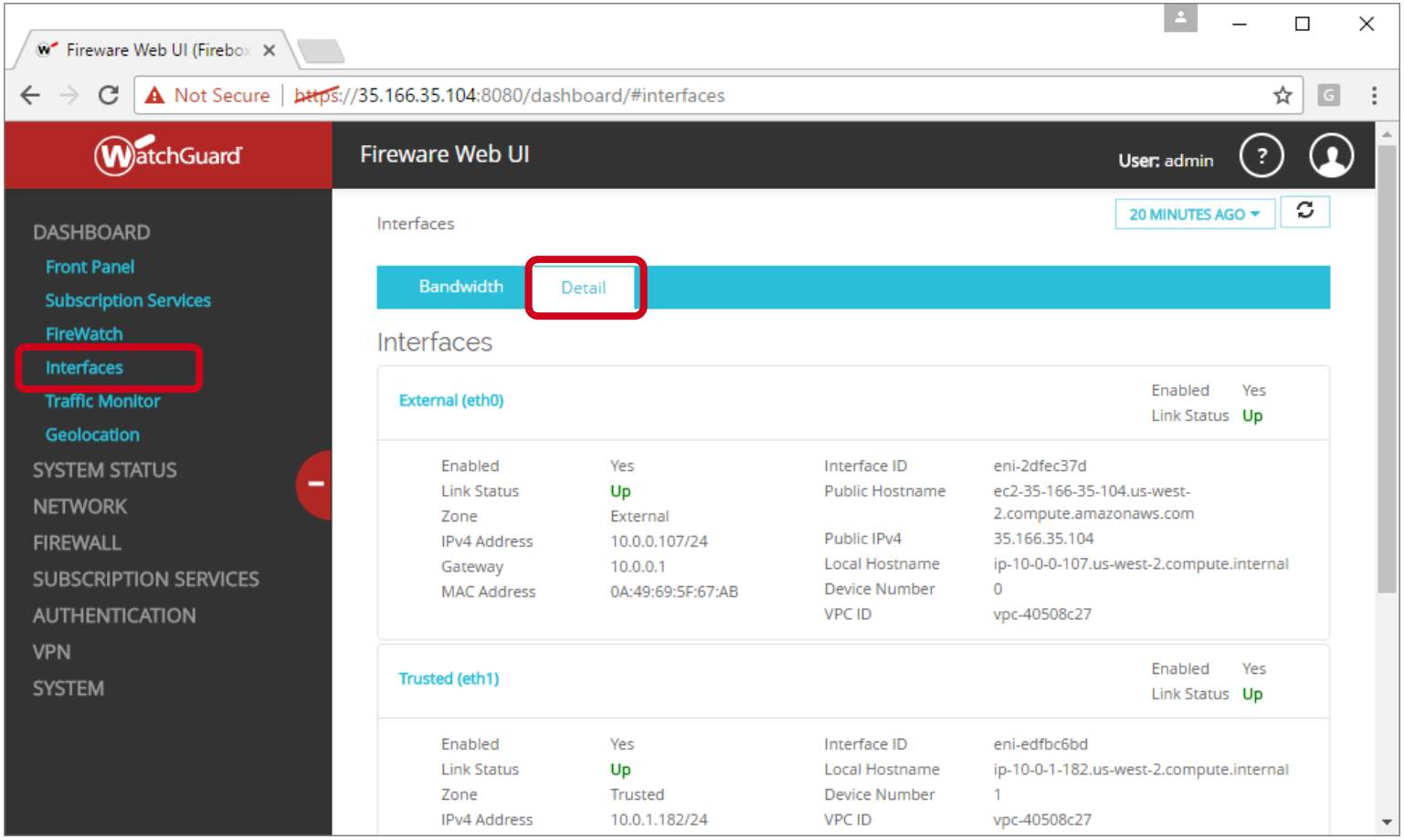
Fireware Web UI für Firebox Cloud

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



Fireware Web UI für Firebox Cloud

- Das **Interfaces** Dashboard zeigt Schnittstellen-konfigurationsinformationen für die Firebox Cloud-Instanz



Live Demo – Firebox Cloud AWS

Vielen Dank!

WatchGuard Training

NOTHING GETS PAST RED.

WatchGuard Training