Ressourcen Schutz in der Microsoft Cloud - Firebox Cloud for Microsoft Azure

Thomas Fleischmann
Senior Sales Engineer
Central Europe

WatchGuard Training

Agenda

- Firebox Cloud Overview
- Fireware OS and Management
- Licensing and Services
- Feature Differences from other Fireboxes
- Deployment Overview
- Fireware Web UI
- Default Configuration

Firebox Cloud Features

- Runs the same Fireware OS as other Fireboxes
- Protects a virtual network from attacks such as botnets, cross-site scripting, SQL injection attempts, and other intrusion vectors
- Enables secure VPN connections to a virtual network
- Compatible with Dimension for monitoring and reporting

Primary Use Cases

- Protect a server on a virtual network
  - Firewall
  - Security services
- Branch Office VPN (BOVPN) endpoint
  - VPN endpoint for encrypted connections between other networks and a virtual network
- Mobile VPN
  - VPN endpoint for encrypted connections from SSL, L2TP, IPSec, or IKEv2 mobile VPN clients to a virtual network

Firebox Cloud Licensing — Azure

- Firebox Cloud for Azure support
  - Bring your own license (BYOL)
  - Pay as you go (PAYG)

- The Firebox Cloud model license you purchase specifies the maximum number of CPU Cores your Firebox Cloud can use

Firebox Cloud Model	Maximum CPU Cores
Small	2
Medium	4
Large	8
Extra Large	16

Firebox Cloud — Instance Sizes

- Recommended instance sizes for Firebox Cloud depend on the Firebox Cloud model

Model	Instance Sizes for Azure	Instance Sizes for AWS
Small	Standard_A1_v2, Standard_A2_v2, Standard_D2_v3, Standard_D2s_v3, Standard_F1, Standard_F2, Standard_F2s_v2	c4.large, m4.large
Medium	Standard_A4_v2, Standard_D4_v3, Standard_D4s_v3, Standard_F4, Standard_F4s_v2	c4.xlarge, m4.xlarge
Large	Standard_A8_v2, Standard_D8_v3, Standard_D8s_v3, Standard_F8, Standard_F8s_v2	c4.2xlarge, m4.2xlarge
Extra Large	Standard_D16_v3, Standard_D16s_v3, Standard_F16, Standard_F16s_v2	c4.4xlarge, m4.4xlarge

Administration

- Administer Firebox Cloud with Fireware Web UI, CLI, or Dimension Command (requires Fireware 12.1 or higher)
- Since Version 12.2 you can administer Firebox Cloud with WatchGuard System Manager, Policy Manager, or WatchGuard Management Server
- Limited Web Setup Wizard
  - Firebox Cloud uses a default configuration

Included Subscription Services

- Application Control
- WebBlocker
- Gateway AV
- APT Blocker
- Intrusion Prevention Service (IPS)
- Reputation Enabled Defense
- Geolocation
- Botnet Detection
- Data Loss Prevention
- Threat Detection and Response (TDR)
- spamBlocker and Quarantine Server (requires Fireware v12.2 or higher)
- Access Portal (requires Fireware v12.1 or higher)

Feature Differences from Other Fireboxes

- Networking features not supported:
  - 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

Feature Differences from Other Fireboxes

- Policy and Security Services not supported:
  - Explicit-proxy and Proxy Auto-Configuration (PAC) files
  - Quotas
  - DNSWatch
  - Network Discovery
  - Mobile Security
- Authentication features not supported:
  - Hotspot

Feature Differences from Other Fireboxes

- System Administration features not supported:
  - Logon disclaimer for device management connections
  - USB drive for backup and restore
- Other features not supported:
  - Gateway Wireless Controller
  - Mobile VPN with SSL **Bridge VPN Traffic** option

Network Interface Configuration

- Firebox Cloud supports up to 8 interfaces
  - 1 external
  - Up to 7 internal
- All interfaces use DHCP to request an IP address
  - There are no interface settings in Fireware Web UI
- You configure all network interface settings in Azure
  - For each additional interface, you must configure the subnet, route table, and interface for the Firebox Cloud VM

Deployment Overview — Azure

- To deploy Firebox Cloud on Microsoft Azure you must:
  1. Create a key pair for SSH authentication
  2. Deploy the Firebox Cloud instance
  3. Activate your Firebox Cloud license
  4. Add the feature key

  For more information, see the *Firebox Cloud Deployment Guide*

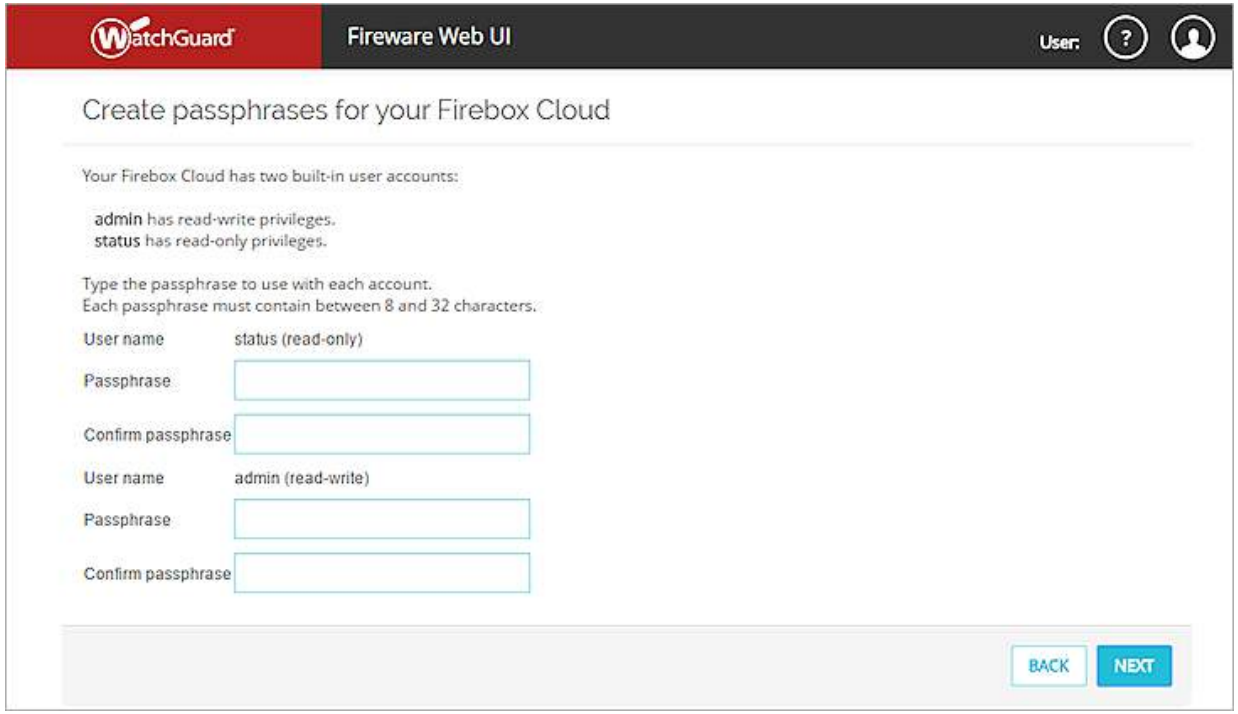
  (https://www.watchguard.com/help/docs/fireware/12/en-US/Firebox-Cloud_Deployment-Guide.pdf)
- Connect to Fireware Web UI at the eth0 public IP address of your Firebox

Deployment Overview — Azure

- To find the Firebox Cloud Instance ID:
  - In the Azure left navigation menu, select Storage accounts.
  - Click the name of the storage account associated with your Firebox Cloud instance.
  - In the Blob Service list, select Containers.
  - Find the boot diagnostic container.The name of the boot diagnostic container is in the format:
  - <bootdiagnostics>-<vmname>-<vmid>

Firebox Cloud Setup Wizard

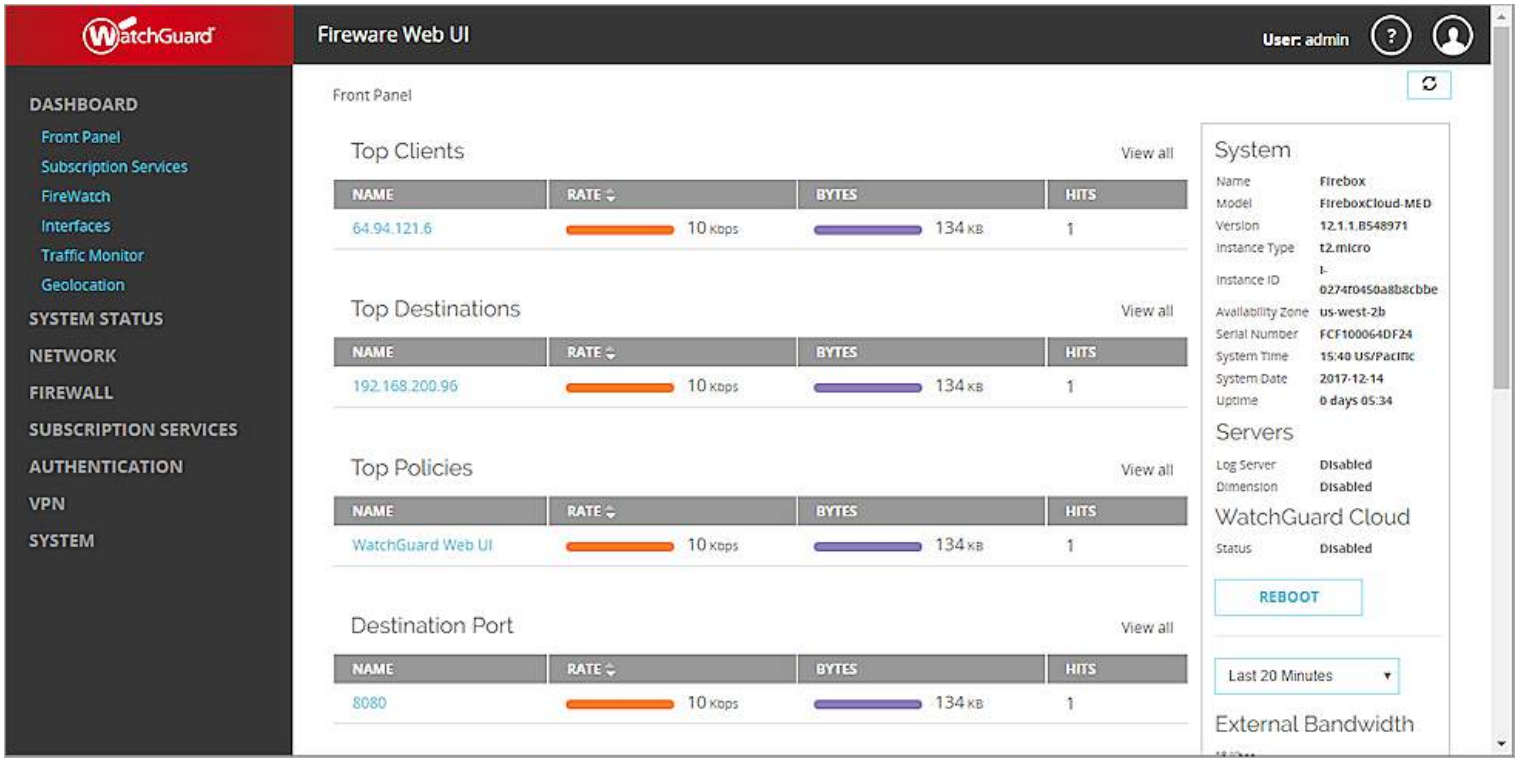
- The first time you connect, the Web Setup Wizard appears
  - Create new passphrases for the built-in user accounts
  - Log in again with the new passphrase



Connect to Fireware Web UI

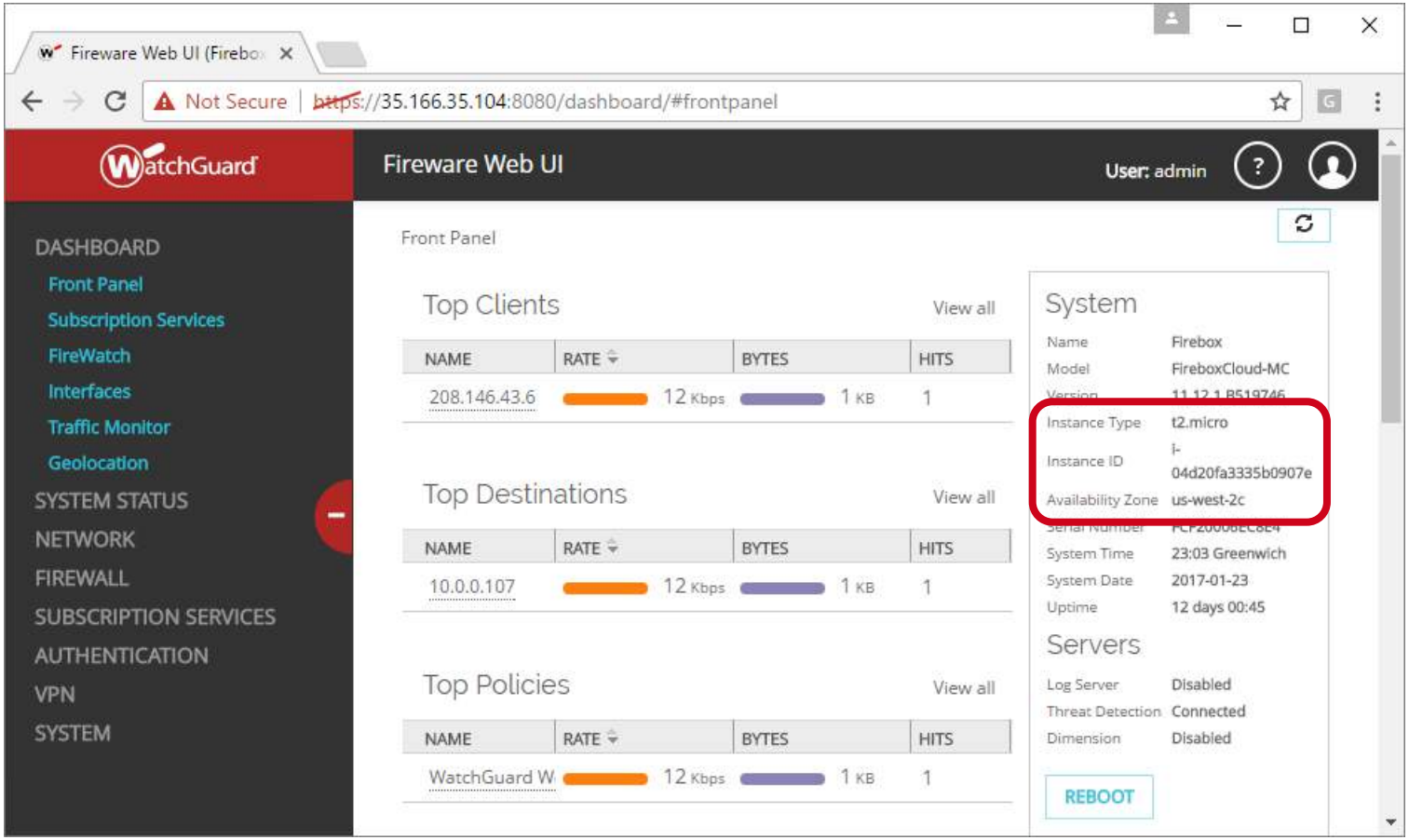
- Connect to Fireware Web UI at the external IP address of your Firebox Cloud

```
https://<eth0_Public_IP>:8080
```



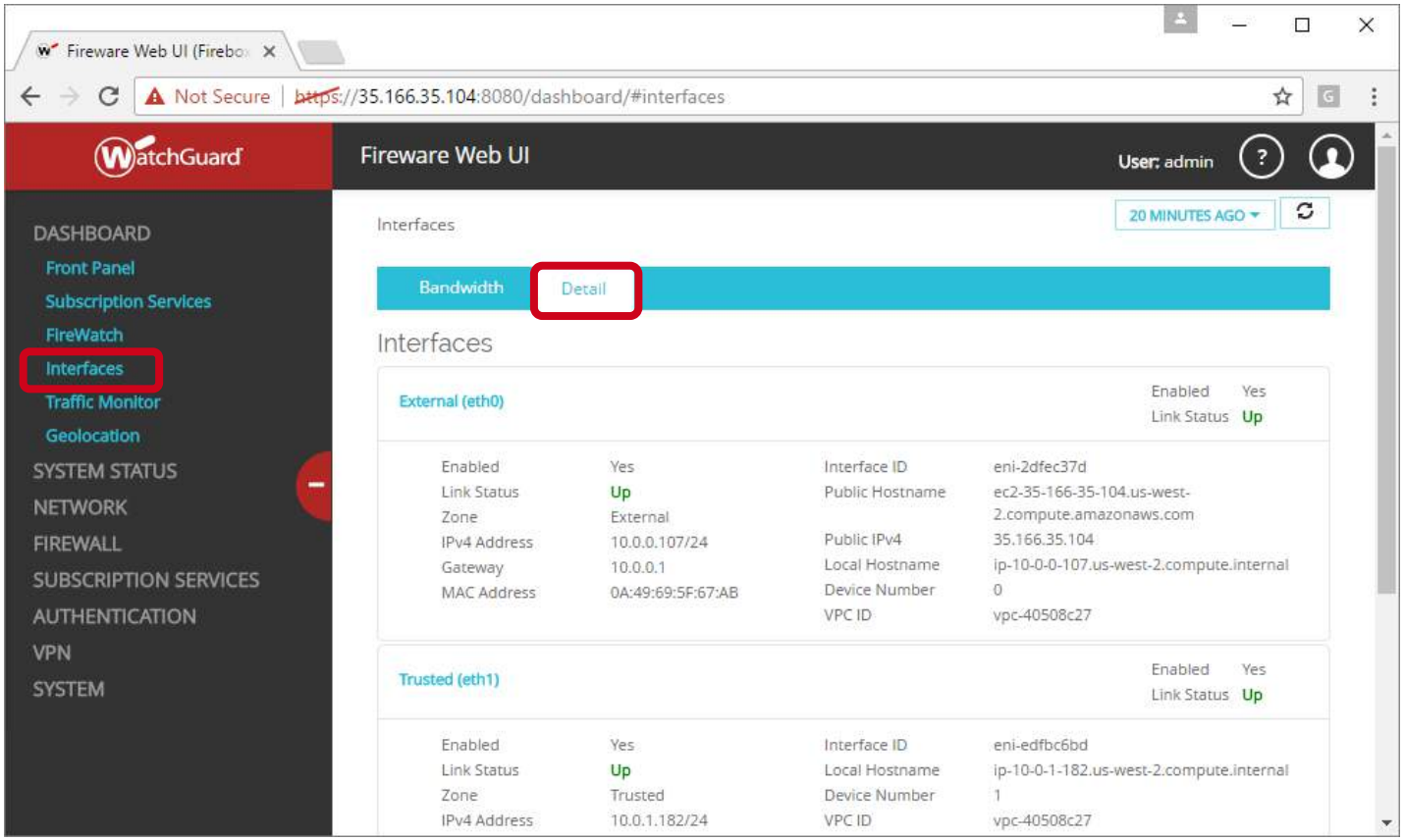
Fireware Web UI for Firebox Cloud

- The **Front Panel** Dashboard page shows instance information



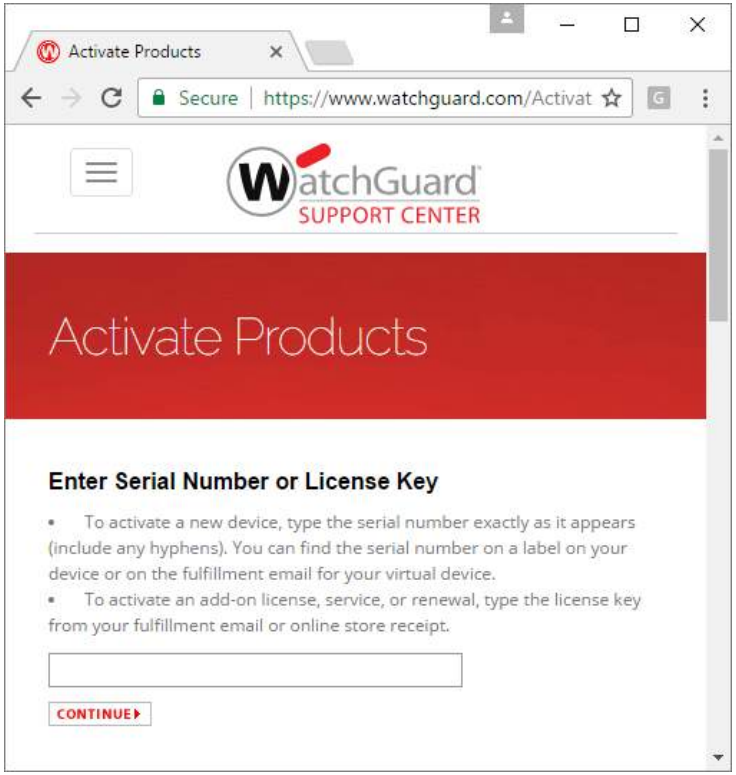
Fireware Web UI for Firebox Cloud

- The **Interfaces** Dashboard page shows interface configuration information for the Firebox Cloud instance



Add a Feature Key

- When you purchase Firebox Cloud, you get a serial number
- After you deploy Firebox Cloud, activate the serial number in the WatchGuard Portal
  - To activate, specify the serial number and the Firebox Cloud Instance ID (VM ID)
  - The activation process generates a feature key for that instance
  - You can apply the feature key only to a Firebox Cloud instance with the specified instance ID

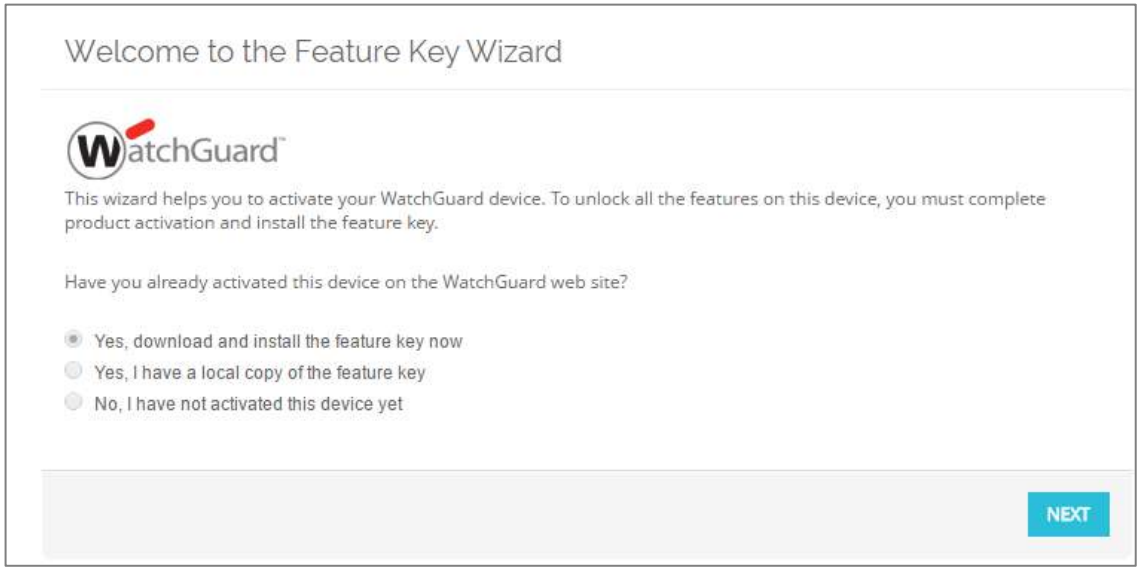


Add a Feature Key

- Download the feature key to the Firebox to enable all features

1. In Fireware Web UI, click **Add a feature key now**

2. The wizard can download and install the feature key

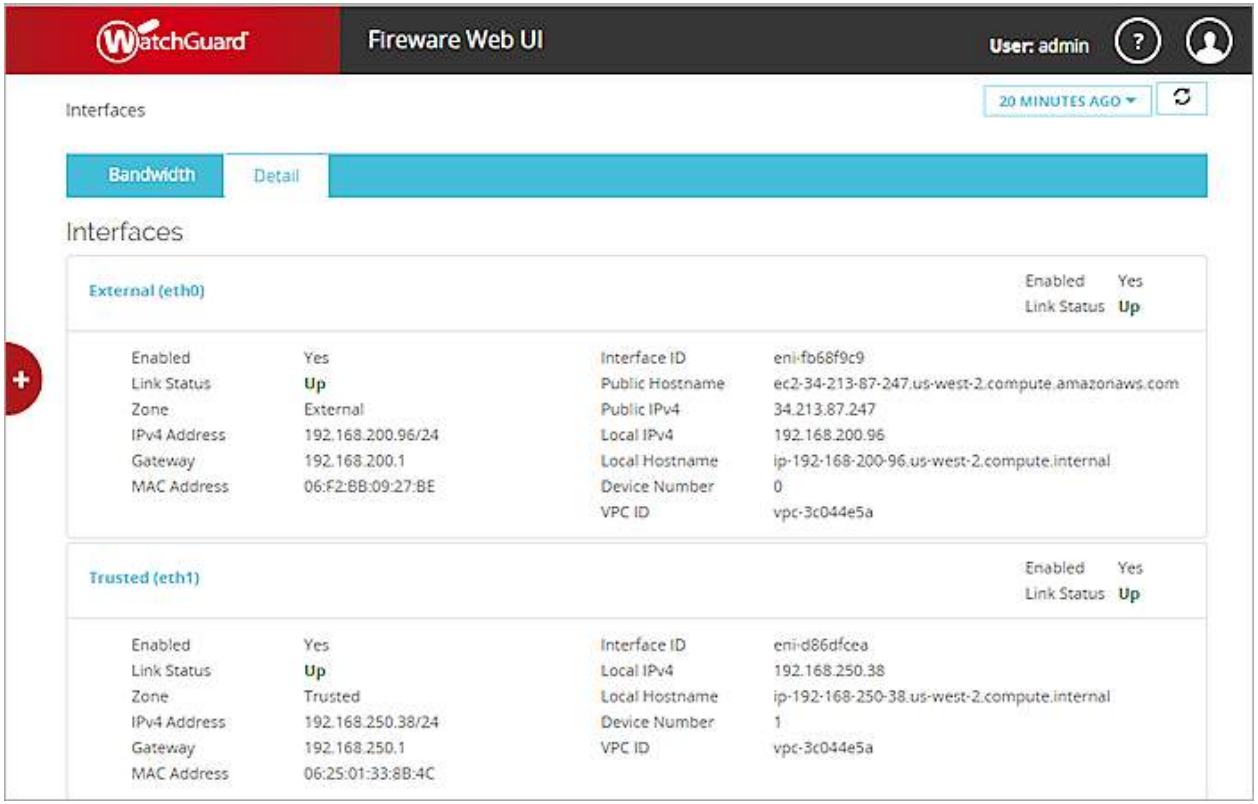


Default Configuration — User Accounts

- Default user accounts are the same as for any other Firebox
  - Device Administrator account:
    - User name — admin
    - Passphrase — *<the Firebox Cloud VM or Instance ID>*
  - Device Monitor account:
    - User name — status
    - Passphrase — readonly
- You change these default passphrases in the Web Setup Wizard when you connect to Firebox Cloud the first time
- You can also select **System > Users and Roles** to change the passphrases for these user accounts

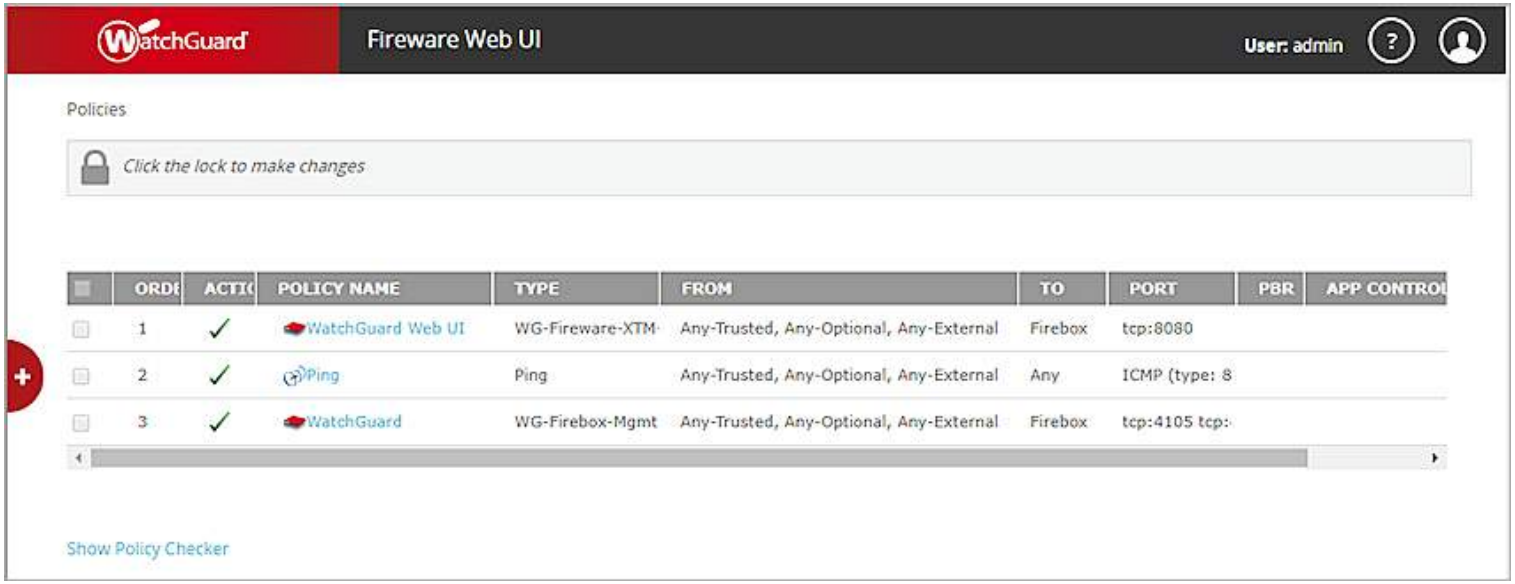
Default Configuration — Interfaces

- Interface 0 — External, IP address assigned through DHCP
- Interface 1 — Trusted, IP address assigned through DHCP



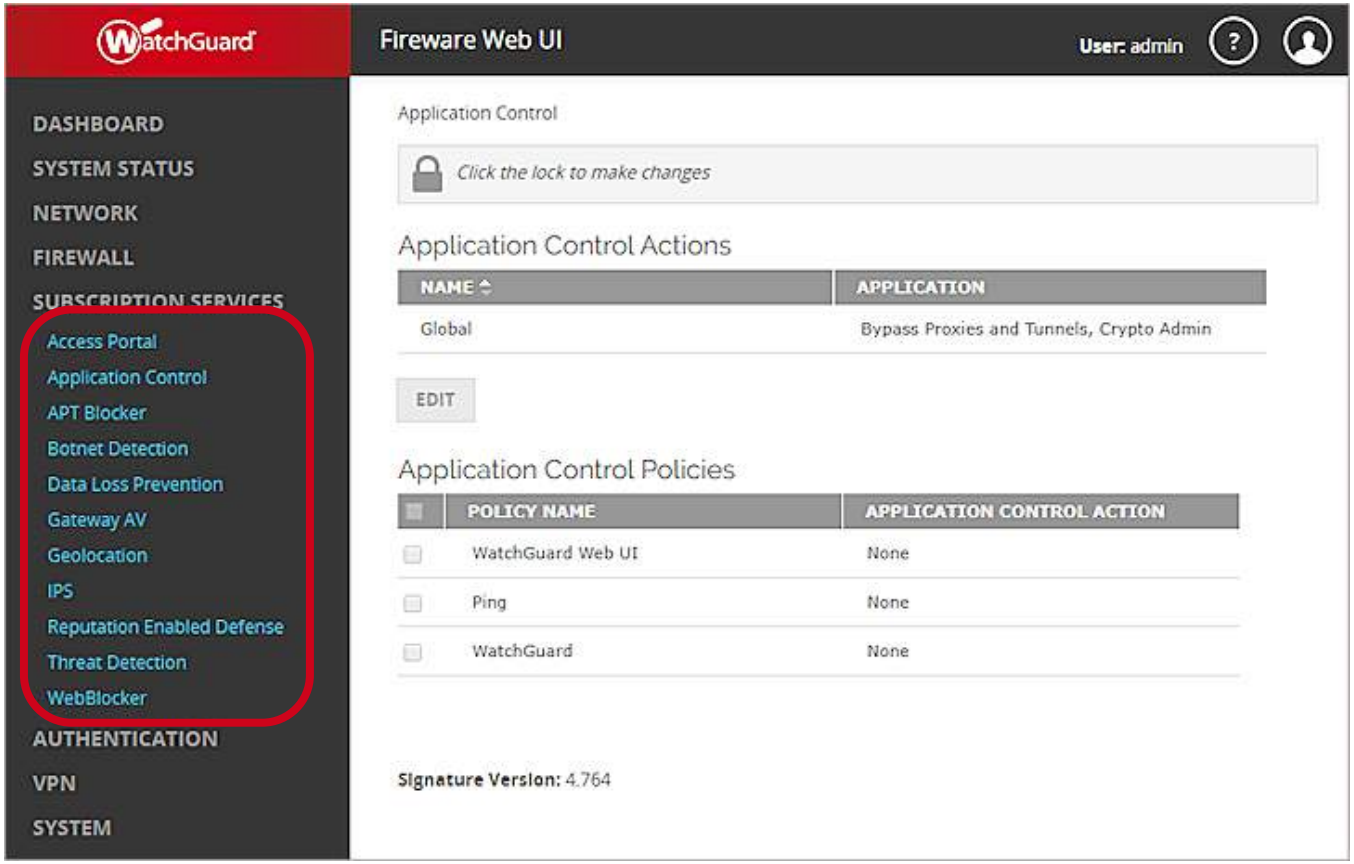
Default Configuration — Firewall Policies

- **WatchGuard Web UI** — Allows Web UI management connections from any interface to the Firebox
- **Ping** — Allows ping traffic from any interface to the Firebox
- No **Outgoing** policy by default — The Firebox does not allow outbound connections unless you configure a policy to allow it



Default Configuration — Services

- Supported subscription services are all configurable, but are not enabled by default



More Information

- For more information about how to deploy Firebox Cloud, see the *Firebox Cloud Deployment Guide*
- For more information about how to configure Fireware features, see Fireware Help

Demo