



Ressourcen Schutz in der Microsoft Cloud

- Firebox Cloud for Microsoft Azure

Thomas Fleischmann
Senior Sales Engineer
Central Europe

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 Firewall v12.2 or higher)
- Access Portal (requires Firewall 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

The screenshot shows the WatchGuard Fireware Web UI interface. At the top, there is a red header with the WatchGuard logo and 'Fireware Web UI'. On the right, there is a 'User:' label with a question mark icon and a user profile icon. The main content area is titled 'Create passphrases for your Firebox Cloud'. Below the title, it states: 'Your Firebox Cloud has two built-in user accounts:'. It lists two accounts: 'admin has read-write privileges.' and 'status has read-only privileges.'. Below this, it says: '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 'Passphrase' and 'Confirm passphrase'. The second set is for the 'admin (read-write)' user, also with fields for 'Passphrase' and 'Confirm passphrase'. At the bottom right, there are two buttons: 'BACK' and 'NEXT'.

Connect to Firewall Web UI

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

`https://<eth0_Public_IP>:8080`

The screenshot displays the WatchGuard Fireware Web UI interface. The left sidebar contains navigation menus for Dashboard, System Status, Network, Firewall, Subscription Services, Authentication, VPN, and System. The main content area is titled 'Front Panel' and features several data tables and a system information panel.

Top Clients

NAME	RATE	BYTES	HITS
64.94.121.6	10 kbps	134 kB	1

Top Destinations

NAME	RATE	BYTES	HITS
192.168.200.96	10 kbps	134 kB	1

Top Policies

NAME	RATE	BYTES	HITS
WatchGuard Web UI	10 kbps	134 kB	1

Destination Port

NAME	RATE	BYTES	HITS
8080	10 kbps	134 kB	1

System Information

Name	Firebox
Model	FireboxCloud-MED
Version	12.1.1.B548971
Instance Type	t2.micro
Instance ID	i-0274r0450a8b8cbb6
Availability Zone	us-west-2b
Serial Number	FCF100064DF24
System Time	15:40 US/Pacific
System Date	2017-12-14
Uptime	0 days 05:34

Servers

Log Server	Disabled
Dimension	Disabled

WatchGuard Cloud

Status	Disabled
--------	----------

Buttons: REBOOT, Last 20 Minutes (dropdown), External Bandwidth

Fireware Web UI for Firebox Cloud

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

The screenshot displays the Fireware Web UI Front Panel dashboard. The interface includes a navigation sidebar on the left with categories like DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'Front Panel' and features three summary tables: 'Top Clients', 'Top Destinations', and 'Top Policies'. Each table lists IP addresses, data rates, and hit counts. On the right side, a 'System' information panel is visible, containing details such as Name, Model, Version, Instance Type, Instance ID, Availability Zone, Serial Number, System Time, System Date, Uptime, Log Server, Threat Detection, and Dimension. A red box highlights the Instance Type (t2.micro), Instance ID (i-04d20fa3335b0907e), and Availability Zone (us-west-2c) fields. A 'REBOOT' button is located 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

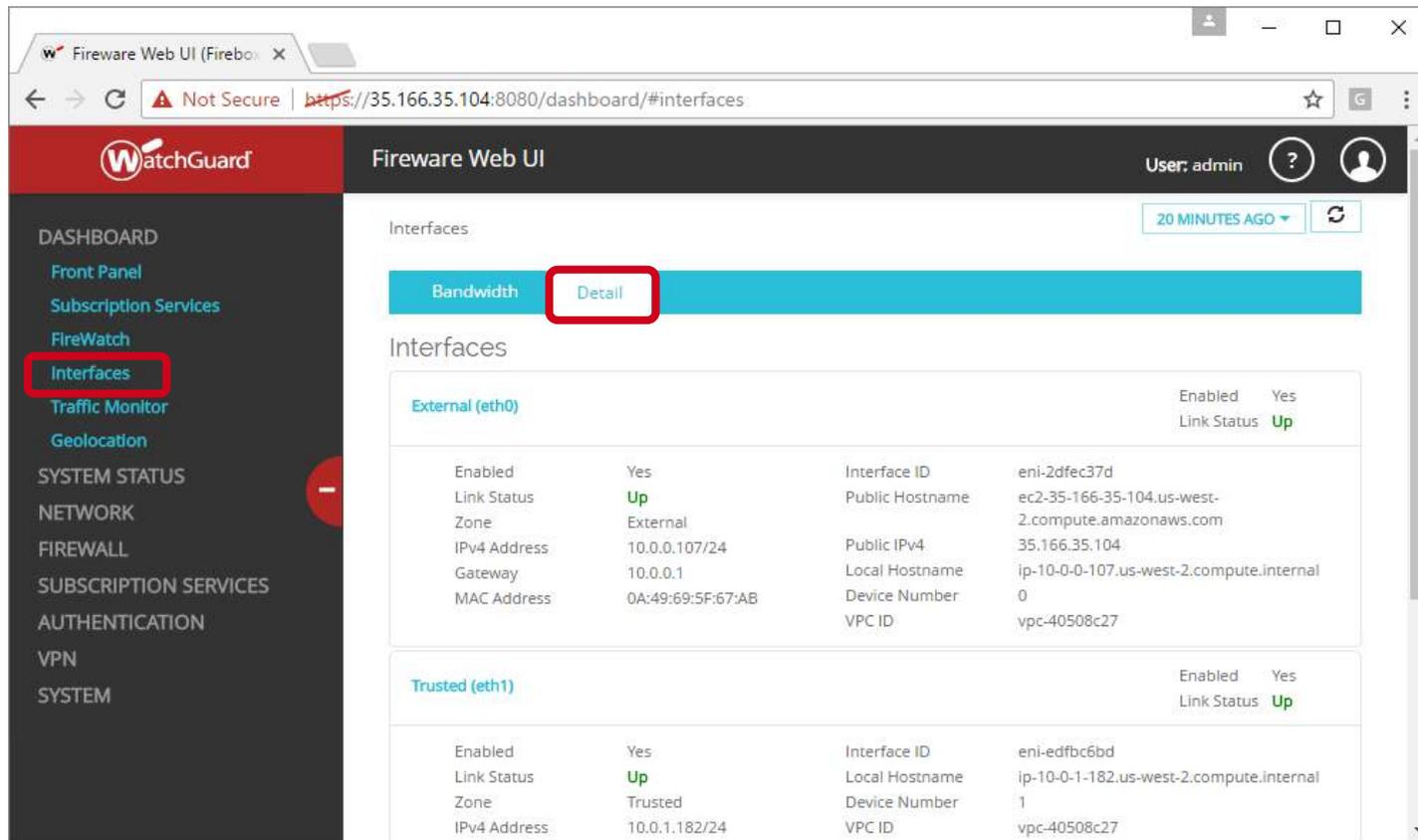
System

Name	Firebox
Model	FireboxCloud-MC
Version	11.12.1.B519746
Instance Type	t2.micro
Instance ID	i-04d20fa3335b0907e
Availability Zone	us-west-2c
Serial Number	FP2000EC8E4
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 for Firebox Cloud

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



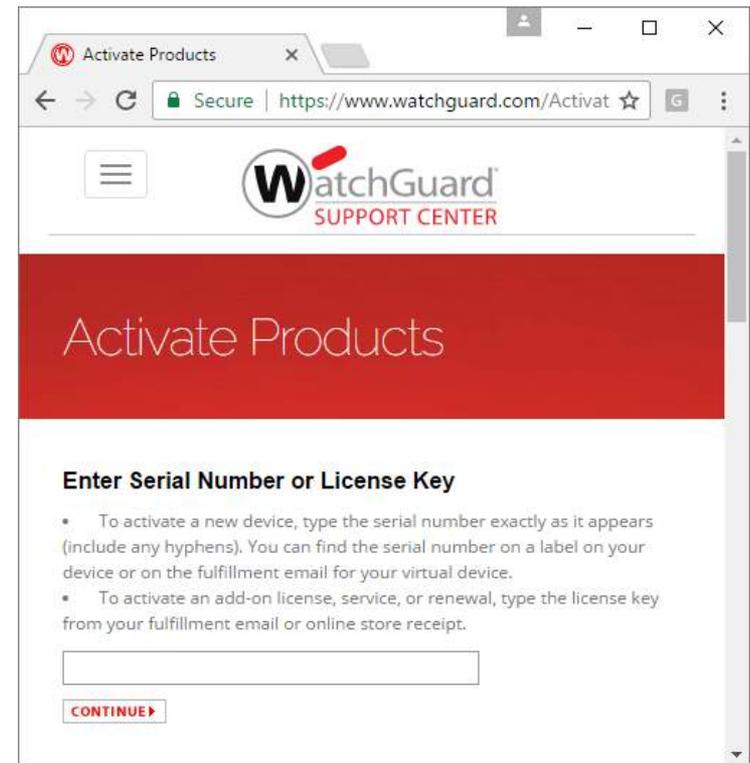
The screenshot displays the Fireware Web UI for Firebox Cloud. The left sidebar contains a navigation menu with the following items: DASHBOARD, Front Panel, Subscription Services, FireWatch, Interfaces (highlighted with a red box), Traffic Monitor, Geolocation, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area shows the 'Interfaces' dashboard. At the top, there are tabs for 'Bandwidth' and 'Detail' (highlighted with a red box). Below the tabs, there are two interface configurations:

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

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

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



The screenshot shows a web browser window with the title 'Activate Products' and the URL 'https://www.watchguard.com/Activat'. The page features the WatchGuard Support Center logo and a red banner with the text 'Activate Products'. Below the banner, there is a section titled 'Enter Serial Number or License Key' with two bullet points: 'To activate a new device, type the serial number exactly as it appears (include any hyphens). You can find the serial number on a label on your device or on the fulfillment email for your virtual device.' and 'To activate an add-on license, service, or renewal, type the license key from your fulfillment email or online store receipt.' A text input field is provided for entering the serial number or license key, and a 'CONTINUE' button is located below the input field.

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

The screenshot displays the WatchGuard Fireware Web UI. The top navigation bar includes the WatchGuard logo, the text "Fireware Web UI", and the user "admin". A refresh button and a timestamp "20 MINUTES AGO" are also visible. The main content area is titled "Interfaces" and has two tabs: "Bandwidth" and "Detail". The "Detail" tab is active, showing a table of interface configurations.

External (eth0)		Enabled	Yes
		Link Status	Up
Enabled	Yes	Interface ID	eni-fb68f9c9
Link Status	Up	Public Hostname	ec2-34-213-87-247.us-west-2.compute.amazonaws.com
Zone	External	Public IPv4	34.213.87.247
IPv4 Address	192.168.200.96/24	Local IPv4	192.168.200.96
Gateway	192.168.200.1	Local Hostname	ip-192-168-200-96.us-west-2.compute.internal
MAC Address	06:F2:8B:09:27:BE	Device Number	0
		VPC ID	vpc-3c044e5a

Trusted (eth1)		Enabled	Yes
		Link Status	Up
Enabled	Yes	Interface ID	eni-d86dfcea
Link Status	Up	Local IPv4	192.168.250.38
Zone	Trusted	Local Hostname	ip-192-168-250-38.us-west-2.compute.internal
IPv4 Address	192.168.250.38/24	Device Number	1
Gateway	192.168.250.1	VPC ID	vpc-3c044e5a
MAC Address	06:25:01:33:8B:4C		

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

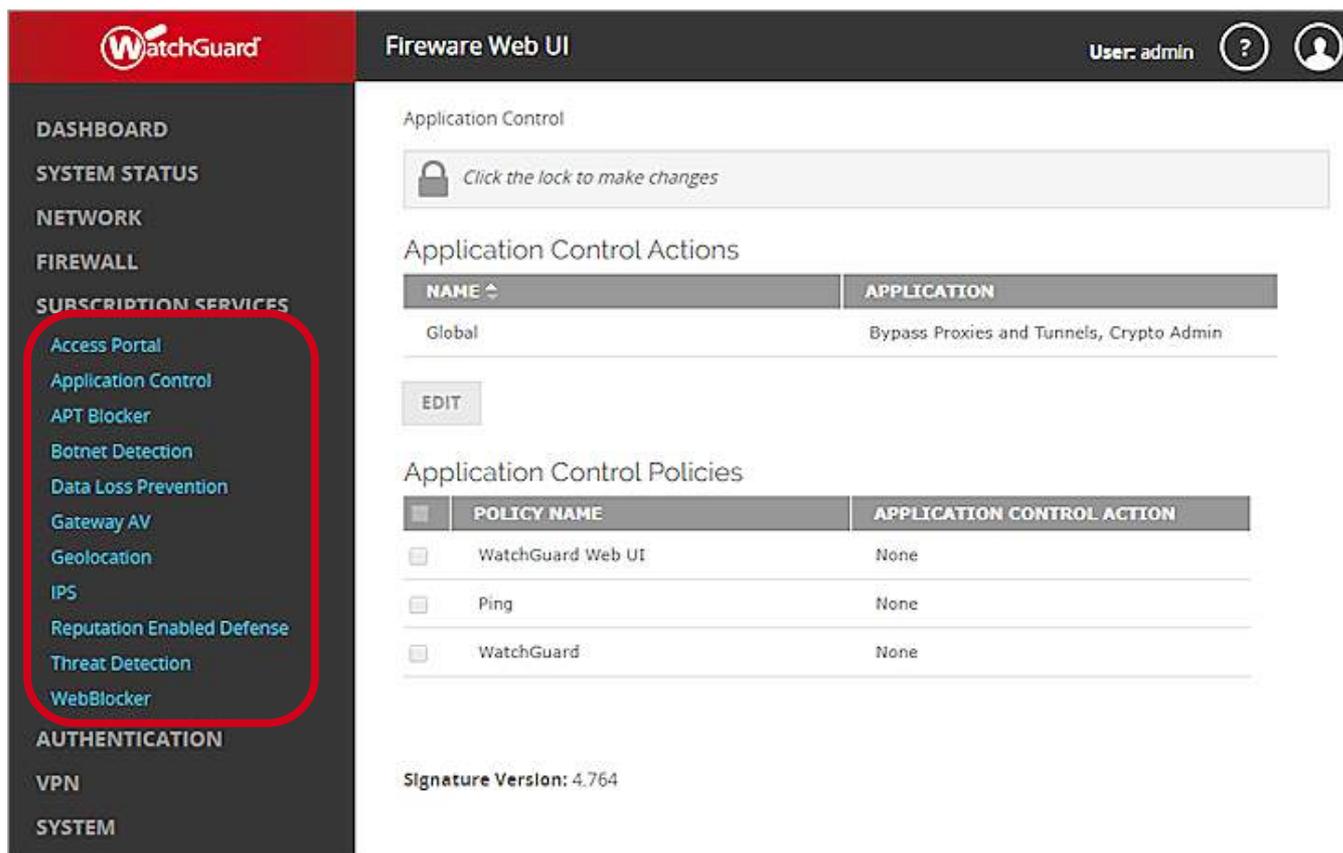
The screenshot shows the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the title "Fireware Web UI", and the user "admin". Below the navigation bar, there is a "Policies" section with a lock icon and the text "Click the lock to make changes". A table lists the default policies:

	ORD#	ACTI	POLICY NAME	TYPE	FROM	TO	PORT	PBR	APP CONTROL
<input type="checkbox"/>	1	✓	WatchGuard Web UI	WG-Fireware-XTM	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:8080		
<input type="checkbox"/>	2	✓	Ping	Ping	Any-Trusted, Any-Optional, Any-External	Any	ICMP (type: 8		
<input type="checkbox"/>	3	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:4105 tcp:		

At the bottom left of the table area, there is a red circular button with a white plus sign. Below the table, there is a "Show Policy Checker" link.

Default Configuration — Services

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



The screenshot displays the WatchGuard Fireware Web UI. The left sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The SUBSCRIPTION SERVICES menu is highlighted with a red rounded rectangle and includes: Access Portal, Application Control, APT Blocker, Botnet Detection, Data Loss Prevention, Gateway AV, Geolocation, IPS, Reputation Enabled Defense, Threat Detection, and WebBlocker. The main content area shows the 'Application Control' configuration page. At the top, it says 'Application Control' and 'User: admin'. Below this is a lock icon and the text 'Click the lock to make changes'. The 'Application Control Actions' section contains a table with two columns: 'NAME' and 'APPLICATION'. The table has one row: 'Global' with the application 'Bypass Proxies and Tunnels, Crypto Admin'. Below the table is an 'EDIT' button. The 'Application Control Policies' section contains a table with two columns: 'POLICY NAME' and 'APPLICATION CONTROL ACTION'. The table has three rows: 'WatchGuard Web UI' with 'None', 'Ping' with 'None', and 'WatchGuard' with 'None'. At the bottom, it says 'Signature Version: 4.764'.

More Information

- For more information about how to deploy Firebox Cloud, see the *Firebox Cloud Deployment Guide*
- For more information about how to configure Firewall features, see [Fireware Help](#)

Demo



Thank You!