

Managed Firewall

Service Description

Conterra allows customers to request changes to device profiles during the Managed Firewall complete customer lifecycle. Customers can request, via the Managed Services Portal, a change of category. Any change implemented through the portal that does not require Conterra to implement the change does not count towards the monthly change quota. The following defines what is considered to be a Firewall policy change:

- Firewall Policy
- Application Control
- Web Filtering
- DNS Filtering

Any change request that varies from the default configuration or Firewall change policy listed above may be completed by Conterra on a time and materials basis. Conterra reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of the Customer's service.

Firewall Policy

Creating a new policy is a two-step process as outlined in this section.

Firewall Policy Step 1

Under the Security tab, select Firewall Objects.



The underlying screen will appear:

FMG/Sales_Engineering	Security Profiles Viser & Device		
🕂 Create 🖨 🧪 Edit <u>व</u> Delete			
□ Name ▼		Details	
FABRIC_DEVICE	Address	IP/MASK: 0.0.0.0/0.0.0.0	any



Select Create + Create then Address

- 1. Enter the name of the asset or category you wish to create a rule around
- 2. Select the Type. Choices are:
 - Subnet .
 - **IP Range** .
 - FQDN
 - Geography .
 - **Device (Mac Address)** .
- 3. Enter the IP/Netmask
- 4. Select Interface (recommend leaving this set as "any")
- 5. Add Comments for easy identification

Select **Save** at the bottom of the screen.



Create New Address Address IPv6 Address Category Name* Color Subnet Type* IP/Netmask* any Interface* Static route configuration Comments Per-Device Mapping



Firewall Policy Step 2

Under the Security tab, select Policy to View, Edit or **Create a New Policy**

Select the applicable device.

Once selected, the existing Firewall Policies will be displayed.



Sale	Enginee	ring/CHRLNCX0LAB	-MRT01/root 🔻 Fi	rewall Policy	~							⊟ 2	Э 🕨
+ Crea	te 🥒 Edi	it 🥫 Delete Actio	n 🗢 🎋 Column Settin	igs 🗮 Policy Block	÷								
		Name	From		Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	N
			🖷 any	🖷 any	🗐 all	🗐 all	🖬 always	🛛 ALL			Q no-inspection	Log All Sessions	



Editing an existing Policy

Editing an existing policy is **not** recommended. Any adjustments to firewall policies should be done via the creation of a new policy. Editing an existing rule may result in conflicts and an increased probability of tickets.

Creating a New Policy

All changes to the Firewall Policy should be done by selecting

Create + Create the key on the page header.

Required field selections to successfully create a firewall policy include:

- Name
- Incoming Interface
- Outgoing Interface
- IPV4 Source
- IPV4 Destination
- Service
- Action

Name

When selecting a Name for your new Policy, be short and as descriptive as possible.

Incoming Interface



The Incoming Interface will always default to "Any," meaning the Policy will be applied to all incoming interfaces. If you need to apply the Policy to specific interfaces, click the dropdown arrow to view all available options. From there, select one or multiple interfaces to which the Policy should apply.

Outgoing Interface

Outgoing Interface

The Outgoing Interface will always default to "Any," meaning the Policy will be applied to all outgoing interfaces. If you need to apply the Policy to specific interfaces, click the dropdown arrow to view all available options. From there, select one or multiple interfaces to which the Policy should apply.

v

ncoming Interface	any X	
Outgoing Interface		
iource Internet Service		
Pv4 Source Address	X III	
Pv6 Source Address		
legate Source		
iource User		
iource User Group		
SSO Groups		
Destination Internet Service		
Pv4 Destination Address	X IIc	
Pv6 Destination Address		
legate Destination		
iervice	ALL X	
ichedule	ahvays X	
Action	Deny Accept	
Disclaimer Options 🔺		
Logging Options A		



IPV4 Source Address

IPv4 Source Address	all X

The IPV4 Source Address will always default to "All," meaning the policy will be applied to all IPV4 sources. If you need to apply the policy to specific IPV4 addresses, click the dropdown arrow to view all available IPV4 source addresses. From there, select one or multiple addresses to which the policy should apply.

IPV4 Destination Address

IPv4 Destination Address	all X	· ►]

The IPV4 Destination Address will always default to "All," meaning the policy will be applied to all IPV4 destinations. If you need to apply the policy to specific IPV4 addresses, click the dropdown arrow to view all available IPV4 destination addresses. From there, select one or multiple addresses to which the policy should apply.

Tip: The Object you created in Step 1 should appear in the drop-down list. Select this if applicable.

Service

Service ALL X Y

The Service setting will always default to "All," meaning the policy will be applied to all services. If you need to apply the policy to specific services, click the dropdown arrow to view all available services. From there, select one or multiple services to which the policy should apply.

Action

Action

🔵 Deny 🛛 Accept

Action indicates whether you are creating the rule to accept or deny traffic. Select the action based on how the rule should be applied.

Comments

The Comments section is a free-form field where you can provide a detailed description of the rule. This description is visible in the Firewall Policy tab, helping you easily identify the rule's purpose. Although optional, including comments is highly recommended.

Finalizing the Policy

At the bottom of the screen, you are given an option to $\ensuremath{\textbf{Cancel}}$ or $\ensuremath{\textbf{Save}}$



- Cancel will return you to the Firewall Policy Tab and all work will be lost
- Save will save the Policy and return you to the Firewall Policy Tab

IMPORTANT – To implement the policy you must select the	🛓 Install 🚺	at the top right of the screen. If not implemented, the
policy will still appear in the Firewall Policy tab but will not be a	ictive.	



Firewall Policy Ordering

Firewall Policies are enforced in order from top to bottom. How they appear on the Firewall Policy Screen will impact the effectiveness of the Firewall.

Sales	_Engineer	ing/CHRLNCX0LAB-	MRT01/root	rewall Policy	·							⊟ 2	Э Ь
+ Creat	e 🥜 Edit	t 🛅 Delete Action	🗢 🌾 Column Settin	gs 🗮 Policy Block 🛊									٩
		Name	From		Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	N
			🖤 any	🖳 any	🗐 all	🚍 all	🐻 always	😨 ALL			Q no-inspection	Log All Sessions	Ø

To change the order of the Firewall Policies, select the policy you wish to change the order of by choosing **Action** then **Move** from the drop-down screen.

- 1. Enter the number of the rule placement currently
- Select **before** or **after**. Select the number from the 2. drop-down box for final placement
- 3. Select Submit

Deleting a Policy

Customer Administrators can delete a Firewall Policy at any time. This can be done by selecting the **applicable policy** from the Firewall Policy Tab.

From #

+ Create	🎤 Edit	Delete Action	• 🎄 Column Settings	; 🗮 Policy Block 🛊						Se	earch	٩
		Name	From		Source	Destination	Schedule	Service	Users	Action	Security Profile	Log
	1		🖬 any	💌 any	🛢 all	🖻 all	🐻 always	😨 ALL		✓ Accept	Q no-inspection	Log All Sessions

And then selecting

The following window will appear. Select the appropriate value.



🛾 🛓 Install 🚺 🗍 **IMPORTANT** – To implement the policy you must select the at the top right of the screen. If not implemented, the policy will remain inactive. It will appear in the Firewall Policy Tab but will not be active.





Application Control

This section outlines the change management options available through the Managed Services Portal. Standard changes are limited to:

- Modifying category treatment to a predefined setting, such as Allow, Block, or Quarantine
- Modifying or adding application overrides
- Modifying or adding filter overrides

Under the Security tab, select Firewall Objects.

Security	^
Policy	
• Firewall Objects	
• Network	
Routing	

The first selection box will default to Address. Leave selection as is. In second selection box, select Application Control.

FMG/Sales_Engineering	 ✓ Security Profiles ✓ User & Device
+ Create 🔹 🎤 Edit 🛛 🗃 Delete	Antivirus Profile Intrusion Prevention Profile
□ Name ◄▲	Ty Local Category
	Ac Web Rating Overrides
	Ac Web Filter Profile
📄 📲 G Suite	Ac Application Control
📄 🌁 Microsoft Office 365	File Filter Profile Ar Video Filter
□ ^Ξ RFC1918-10	SSL/SSH Inspection Ad Profile Group
□	Address

Application Control Profiles assigned to the Firewall can be seen on this screen.

🕂 Create 📝 Edit 🝵 Delete		Search	Q
block-high-risk	2024-07-12 22:32:50	2024-09-11 13:08:47	

For first-time users, this will be one of the three (3) default profiles you selected during your initial activation.

It is highly recommended that users edit the existing profile and not create a new profile.

Select the profile you wish to make changes to and then select Edit

USER GUIDE



Managed Firewall

Categories will appear on the screen with current treatment.

To change treatment, select the desired treatment.

Please note that selecting **"Quarantine"** will only function if the device has available internal storage. The Managed Services Portal does not restrict users from choosing the "**Quarantine"** option in any scenario.

Edit Application Control						
Name* block-high-risk						
Comments						
Category						
General.Interest	Monitor	Allow	Block	Quarantine	Traffic Shaping	Reset
Network.Service	Monitor	Allow	Block	Quarantine	Traffic Shaping	Reset
Update	Monitor	Allow	Block	Quarantine	Traffic Shaping	Reset
P2P	Monitor	Allow	Block	Quarantine	Traffic Shaping	Reset
Email	Monitor	Allow	Block	Quarantine	Traffic Shaping	Reset

Application and Filter Overrides

By default, all application controls are limited to their assigned categories upon initial installation. If an application needs to be treated differently than its defined category, an Application and Filter Override Rule can be created to customize its handling.

Creating an Application Override Rule

Select the action to be applied.

Select the application(s) to apply the rule.

Filters available are:

- Category
- Popularity
- Technology
- Behavior
- Vendor
- Protocols
- Risk

Select all applicable filters.

Application and Filter Overrides			
🕂 Create 🥒 Edit 🛛 🗑 Delete			
Priority Detail			
	-	1	
	No data a	vailable	
20 🗢 entries			
Create New Address			
Category	Address	Pv6 Address	
Name*			
Color			~
Type*	Subnet		
IP/Netmask*			
Interface*	any		~
Static route configuration	•		
Comments			
Per-Device Mapping 🔺			



Creating a Filter Override Rule

Select the action to be applied.

Filters available are:

- • Category
- • Popularity
- Technology
- • Behavior
- Vendor
- Protocols
- •Risk

Select all applicable filters.

Finalizing the Policy

At the bottom of the screen, you are given an option to **Cancel** or **Save**

- Cancel will return you to the Firewall Policy Tab and all work will be lost.
- Save will save the policy and return you to the Firewall Policy Tab.

IMPORTANT – To implement the policy you must select the end of the screen. If not implemented, the policy will remain inactive. It will appear in the Firewall Policy Tab but will not be active.

Web Filter

This section outlines what change management is available through the Managed Services Portal. Standard changes are limited to:

• Modification of Category treatment to a standard defined treatment including Allow & Block

Under the Security tab, select Firewall Objects.



Туре	Application	Filter	
Action	Monitor		~
Category			
General.Interest	Network.Service	Update	
P2P	Email	Storage.Backup	
Social.Media	Web.Client	Industrial	
Collaboration	Business	VoIP	
Cloud.IT	Mobile	Unknown Applications	
Video/Audio	Proxy	Remote.Access	
Game			
Popularity			
1	2		
4			
Technology			
Network-Protocol	Browser-Based	Client-Server	
Peer-to-Peer			

Create New Application and Filter Overrides



The first selection box will default to Address. Leave selection as is. In second selection box, Select Web Filter Profile.

FMG/Sales_Engineering	~	Security Profiles
+ Create 🗢 🎤 Edit 🔋 Delete		Antivirus Profile
□ Name ▼*		Local Category
	A	Web Rating Overrides
FIREWALL_AUTH_PORTAL_ADDRESS	A	Web Filter Profile
📄 🗧 G Suite	A	Application Control
📄 🌁 Microsoft Office 365	A	File Filter Profile Video Filter
□	A	SSL/SSH Inspection Profile Group
□	A	Idress

Web Filtering Profiles assigned to the Firewall can be seen on this screen.

🕂 Create 🕜 Edit 🛛 🗑 Delete						Search	
							Last Modified 💌
🗌 🕈 default	Default web filtering.			Flow-based	2024-07-12 22:32:50		2024-09-11 13:07:55
Edit DNS Filter							
Name*	default						
Comments	Default dns filtering.						
Block DNS requests to known botnet C&C							
Enforce 'Safe search' on Google, Bing, YouTube	•						
dns-filter.category.based.filter							
Allow Monitor dns-filter.redirect.to.blo	ck.portal		Q				
□ Name ▼ ▲							
Drug Abuse		😋 Allow					
Hacking		😋 Allow					
Illegal or Unethical		S Allow					
Discrimination		S Allow					
Explicit Violence		S Allow					
Extremist Groups		Monitor					

For first-time users, this will be one of the three (3) default profiles you selected during your initial activation.

It is highly recommended that users edit the existing profile and not create a new profile.

Select the profile you wish to make changes to and then

select Edit 🖊 Edit

A list of category-based filters will be shown along with the Action.

To change Actions, select the category you want to change and then select the Action you want to be applied.

Section Allow Monitor Block A Warning Authenticate



URL Filtering

There are three Static URL Filters available. Block invalid URLs and Block malicious URLs discovered by sandbox are toggles. They are by default turned off but can be changed by toggling this to ON. When turned on the button next to the category will appear as

dns-filter.static.domain.filter 🔫			
Domain Filter	0		
dns-filter.external.ip.block.lists			
dns-filter.dns.translation	0		

Where specific URLs within a category are allowed or blocked and the desire is to change treatment for only that URL, then Select **URL Filter.**

L Filter	(0	
- Create 🧪 Edit 🛛 💼 Delete			٩
		٥	
		No data available	

By default, there will be no URL filters at installation. Any rules created post-install will appear on this screen. To add a URL filter, select the **Create button**.

Simple	Regular F			
Simple	Regular Ex			
	Regular E	pression	Wildcard	
Exempt	Block	Allow	Monitor	
Enable	Disable			
Cancel		Save		
	Enable	Enable Disable	Enable Disable Cancel Save	Cancel Save



- 1. Type in the URL to create a rule around
- 2. Select the Type
- 3. Choose the Action or treatment desired
- 4. Select the Status:
 - Select Enable if the identified site belongs to a category that is blocked
 - · Select Disable if the identified site belongs to a category that is allowed
- 5. Select Save

IMPORTANT – To implement the filters you must select the *install* at the top right of the screen. If not implemented, the filters will remain inactive. They will appear in the Web Filter Tab but will not be active.

DNS Filter

- · Modification of Category treatment to a standard defined treatment including Allow, Monitor, Block
- Requests for whitelisting or blacklisting of domains

Under the Security tab, select Firewall Objects.



The first selection box will default to Address. Leave selection as is. In the second selection box, Select DNS Filter Profile.





DNS Filter Profiles can be seen on this screen.

FMG/Sales_Engineering Firewall Objects DNS Filter Profile	: Viser & Device V			
+ Create 🖌 Edit 🝵 Delete				
Jefault	Default dns filtering.	2024-07-12 22:32:50	2024-07-12 22:32:50	
20 🖨 entries				

First-time users will have a single DNS Filter profile available. This profile is one of the three identified during installation. To adjust the profile, select Edit real to the three identified during installation.

Edit DNS Filter			
Name*	default		
Comments	Default dns filtering.		
Block DNS requests to known botnet C&C			
Enforce 'Safe search' on Google, Bing, YouTube	•		
dns-filter.category.based.filter			
S Allow Monitor Ødns-filter.redirect.to.blo	ck.portal		
□ Name ▼ ▲			
Drug Abuse		Seallow Seallow	
Hacking		S Allow	
Illegal or Unethical		Second Se	
Discrimination		S Allow	
Explicit Violence		S Allow	
Extremist Groups		@ Monitor	

A list of category based filters will be shown along with the Action.

To change Actions, select the category you want to change and then select the Action you want to be applied.



Static Domain Filters

Enable to define local static domain filters to allow or block specific domains. The local domain filter has a higher priority than the FortiGuard category-based domain filter.

Available options can be viewed towards the bottom of the DNS Filter Profile tab.

dns-filter.static.domain.filter 👻	
Domain Filter	0
dns-filter.external.ip.block.lists	
dns-filter.dns.translation	



Creating a Domain Filter

Toggle the Domain Filter button to appear as

Select Create

🕂 Create 📝 Edit 🛛 💼 Delete

- 1. **Domain:** Enter a domain.
- 2. Type: Select Simple, Regex, or Wildcard.
- 3. Action: Select Block, Allow, or Monitor.
- 4. Status: Enable or Disable this domain filter.
- 5. Select Save

IMPORTANT – To implement the filters you must select the at the top right of the screen. If not implemented, the

Allov

Disable

Cancel

-

Block

Enable

Save

Ins-filter.static.domain.filter

n Filter

Domain Filter

Domain' Type

Action

Status

filters will remain inactive. They will appear in the Web Filter Tab but will not be active.