



CROWDSTRIKE

FALCON FIREWALL TRIAL GUIDE

150 MATHILDA PL SUITE 650, SUNNYVALE, CALIFORNIA 94086

TEL: (888)512-8906 FAX:(949) 417-1289

WWW.CROWDSTRIKE.COM

TABLE OF CONTENTS

3	INTRODUCTION
4	GETTING STARTED
5	CREATING A FIREWALL RULE GROUP
7	EDITING A FIREWALL RULE GROUP
10	CONFIGURING A FIREWALL POLICY
14	APPLYING FIREWALL RULE GROUP TO POLICY
16	ASSIGNING A FIREWALL POLICY TO A HOST GROUP
19	SUMMARY
20	ABOUT CROWDSTRIKE

INTRODUCTION

CrowdStrike® Falcon Firewall Management™ makes it easy to manage host firewalls that are native to the operating system, simplifying creation, enforcement and maintenance of firewall policies. Falcon Firewall Management enhances protection from network threats by eliminating the visibility gaps and complexity often associated with host firewalls.

Delivered via the same lightweight CrowdStrike Falcon® agent and cloud-delivered architecture, Falcon Firewall Management deploys and is operational in minutes with little impact on the host — from initial enablement to ongoing day-to-day use.

This user guide allows you to see the value of the host firewall management in context with the rest of the Falcon interface. Through this guide you will explore a few use cases for the Falcon Firewall Management module that help you easily create, enforce and maintain firewall rules, rule groups and policies with a simple, centralized approach.



Falcon Firewall Management provides simple, centralized firewall management, making it easy to manage and enforce host firewall policies.

GETTING STARTED

In this guide we'll introduce you to the firewall management process. The guide will get you started — for a more in-depth understanding of the Firewall configuration options, refer to the [Firewall Management documents](#) in the Falcon console.

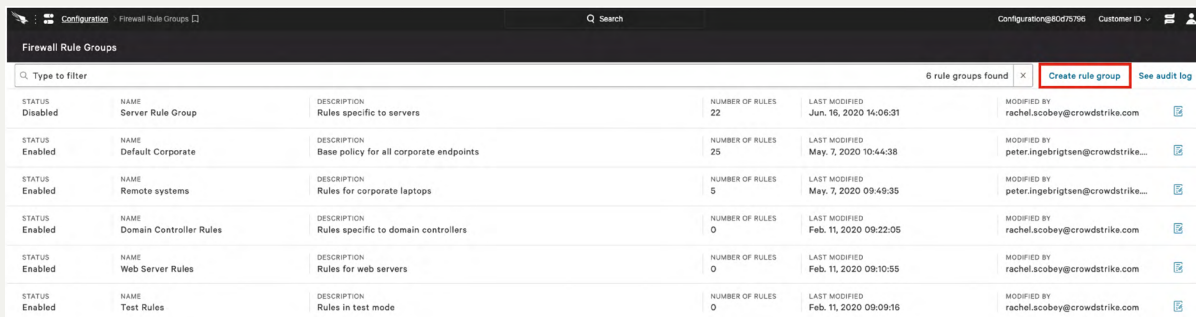
After logging in to the CrowdStrike user interface (UI), you can access Falcon firewall groups and policies in the Configuration App. Managing the firewall features consists of three components: a firewall rule, a firewall rule group and a firewall policy. The individual firewall rules are applied to firewall groups. Once the groups have been created, they can be combined in different ways to create unique firewall policies.

To get started, click on the falcon and navigate to “Firewall Rule Groups.”

The screenshot displays the CrowdStrike Falcon console interface. The top navigation bar includes the 'Activity' tab, a search bar, and user information. The left sidebar contains various navigation options categorized into Bookmarks, Activity, Investigate, Hosts, Configuration, Dashboards, Discover, Spotlight, Intelligence, MalQuery, Users, and CrowdStrike Store. The 'Configuration' section is expanded, showing options like Prevention Policies, Custom IOA Rule Groups, Detection Activity, Detection Resolution, Audit App, Sensor Dashboard, Pay-As-You-Go Usage, Firewall Policies, Firewall Rule Groups (highlighted with a red box), USB Device Policies, Response Policies, Response Scripts & Files, Containment Policy, Sensor Update Policies, and General Settings. The main content area shows a table of detection events with columns for Tactic & Technique, Detect Time, and Host. Below the table, there are sections for 'Monitor Windows CPU and RAM capacity in Falcon Discover' and 'Search for Intel data in Falcon'. At the bottom, there are release notes for Falcon X reports, Windows 5.38.11809 sensor, and prioritized remediations in Spotlight.

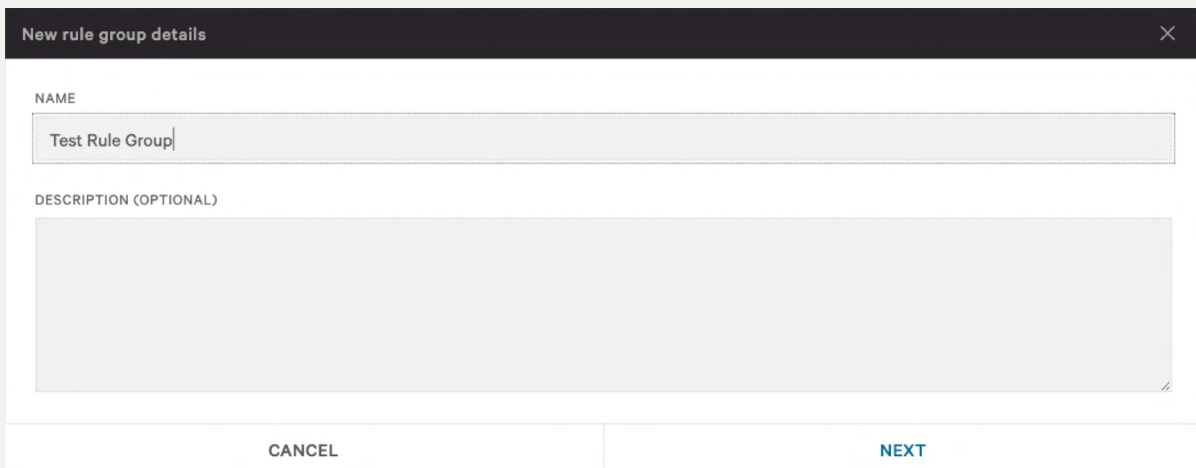
CREATING A FIREWALL RULE GROUP

On the Firewall Rule Groups page, click the Create Rule Group button in the upper right-hand corner.



Firewall Rule Groups					
Type to filter					
6 rule groups found					
STATUS Disabled	NAME Server Rule Group	DESCRIPTION Rules specific to servers	NUMBER OF RULES 22	LAST MODIFIED Jun. 16, 2020 14:06:31	MODIFIED BY rachel.scobey@crowdstrike.com
STATUS Enabled	NAME Default Corporate	DESCRIPTION Base policy for all corporate endpoints	NUMBER OF RULES 25	LAST MODIFIED May. 7, 2020 10:44:38	MODIFIED BY peter.ingebrigtson@crowdstrike...
STATUS Enabled	NAME Remote systems	DESCRIPTION Rules for corporate laptops	NUMBER OF RULES 5	LAST MODIFIED May. 7, 2020 09:49:35	MODIFIED BY peter.ingebrigtson@crowdstrike...
STATUS Enabled	NAME Domain Controller Rules	DESCRIPTION Rules specific to domain controllers	NUMBER OF RULES 0	LAST MODIFIED Feb. 11, 2020 09:22:05	MODIFIED BY rachel.scobey@crowdstrike.com
STATUS Enabled	NAME Web Server Rules	DESCRIPTION Rules for web servers	NUMBER OF RULES 0	LAST MODIFIED Feb. 11, 2020 09:10:55	MODIFIED BY rachel.scobey@crowdstrike.com
STATUS Enabled	NAME Test Rules	DESCRIPTION Rules in test mode	NUMBER OF RULES 0	LAST MODIFIED Feb. 11, 2020 09:09:16	MODIFIED BY rachel.scobey@crowdstrike.com

Give the new rule group a name and description.



New rule group details

NAME

Test Rule Group

DESCRIPTION (OPTIONAL)

CANCEL

NEXT

Define which rules you'd like to have in the new rule group. There are options to start with no rules, with a rule group you've previously created or with a set of predefined rules supplied by CrowdStrike.

New rule group details

Start with an empty rule group or an existing rule group

☐ Empty rule group
 ☐ Rule group you've created
 ☒ CrowdStrike preset rule groups

GO BACK

NEXT

If you select either the CrowdStrike rule group or the rules previously created by your organization, the next window will allow you to select which specific rules groups you'd like in the new group. Select "Create Rule Group" after making your selection.

New rule group details

Select a CrowdStrike preset rule group to copy

	Name ▾	Description	Number of rul...	Status ▾	Last modif... ▲	Modified by ▾
☐	Relaxed Wind...	Windows rela...	1	Disabled	Aug. 19, 2020 ...	CrowdStrike
☒	Core Windows...	Windows core...	21	Disabled	Aug. 19, 2020 ...	CrowdStrike

LOAD MORE

GO BACK

CREATE RULE GROUP

The rule group has now been created, and you're ready to move on to your next step. If you'd like to explore this more, refer to [the documentation for rules and rule groups](#).

EDITING A FIREWALL RULE GROUP

The newly created group page has four primary sections, as labeled in the screenshot below. The Create New Rule button is indicated by the number “1.” Also listed here is the Edit Precedence toggle, which can be used after multiple rules have been created. The section labeled “2” is a list of the rules that currently exist in the rule group. “3” refers to the three tabs in the upper left corner: Rules, Firewall Policies and Audit Log. Finally, “4” indicates the buttons that allow you to cancel, save and delete changes. The Enable Group button will have to be clicked after all changes have been saved, and you’re ready to move to the next step.

The screenshot displays the Falcon Firewall interface for editing a rule group. The top navigation bar shows 'All Firewall Rule Groups' and 'Test Rule Group (Disabled)'. Below this, there are three tabs: 'RULES', 'FIREWALL POLICIES', and 'AUDIT LOG'. The 'RULES' tab is active, showing a list of rules. The 'Rule group details' section at the top right indicates the group is 'Disabled'. The 'Create new rule' button is located at the bottom right of the table. The table itself contains 10 rules, each with a unique precedence number and a status of 'Enabled'.

Precedence	Status	Rule name	Description	Traffic direc...	Action to take	Protocol	Local Address	Local port	Remote IP	Remote port	Executable f...	Location	Actions
1	Enabled	Receive ICM...	Allow ICMPv...	In	Allow	ICMPv6	*		*		System	Any	[Edit]
2	Enabled	Receive ICM...	Allow ICMPv...	In	Allow	ICMPv4	*		*		System	Any	[Edit]
3	Enabled	DHCP on IPv4	Allow DHCP ...	Both	Allow	UDP	*	68	*	67	%SystemRoo...	Any	[Edit]
4	Enabled	DHCP on IPv6	Allow DHCP ...	Both	Allow	UDP	*	546	*	547	%SystemRoo...	Any	[Edit]
5	Enabled	Internet Gro...	Allow IGMP ...	Both	Allow	2	*		*		System	Any	[Edit]
6	Enabled	ICMPv6 Mul...	Allow ICMPv...	Both	Allow	ICMPv6	*		*		System	Any	[Edit]
7	Enabled	ICMPv6 Mul...	Allow ICMPv...	Both	Allow	ICMPv6	*		*		System	Any	[Edit]
8	Enabled	ICMPv6 Mul...	Allow ICMPv...	Both	Allow	ICMPv6	*		*		System	Any	[Edit]
9	Enabled	ICMPv6 Mul...	Allow ICMPv...	Both	Allow	ICMPv6	*		*		System	Any	[Edit]
10	Enabled	ICMPv6 Nel...	Allow ICMPv...	Both	Allow	ICMPv6	*		*		System	Any	[Edit]

To add a new firewall rule, click the Create New Rule button.

Add new firewall rule

NAME

DESCRIPTION (OPTIONAL)

PLATFORM

Windows

ADDRESS FAMILY

IPv4

PROTOCOL

Any

LOCAL ADDRESS

e.g. 192.0.2.0; 192.0.2.0/24; 192.0.2.0-1

REMOTE ADDRESS

e.g. 192.0.2.0; 192.0.2.0/24; 192.0.2.0-1

ACTION

Allowed

DIRECTION

Inbound and outbound

WATCH MODE

☐ Create events for this rule and show rule matches in Activity > Firewall, the Firewall API, and the streaming API. Recommended only for critical rules and troubleshooting.

NETWORK PROFILE

× Any

EXECUTABLE FILEPATH

C:, \\server\sharename, or %systemroot%, then \directory\file.exe

SERVICE NAME

CANCEL

ADD FIREWALL RULE

After configuring your new firewall rule, click Add Firewall Rule.

The new firewall rule will appear at the bottom below any previously existing rules.

All Firewall Rule Groups Test Rule Group (Disabled)													
Unsaved changes on the rules tab													
☐	PREC...	12	Enabled	ICMPv6 F...	Allow ICM...	Both	Allow	ICMPv6	*		*		System Any
☐	PREC...	13	Enabled	ICMPv6 P...	Allow ICM...	Both	Allow	ICMPv6	*		*		System Any
☐	PRE...	14	Enabled	ICMPv6 R...	Allow ICM...	In	Allow	ICMPv6	*		fe80::/64		System Any
☐	PREC...	15	Enabled	ICMPv6 R...	Allow ICM...	Out	Allow	ICMPv6	fe80::/64		*		System Any
☐	PRE...	16	Enabled	ICMPv6 R...	Allow ICM...	Both	Allow	ICMPv6	*		*		System Any
☐	PREC...	17	Enabled	ICMPv6 T...	Allow ICM...	Both	Allow	ICMPv6	*		*		System Any
☐	PRE...	18	Enabled	Lsass	Allow TC...	Out	Allow	TCP	*		*		%System... Domain
☐	PRE...	19	Enabled	Microsoft ...	Allow TC...	Out	Allow	TCP	*		*	445	System Domain
☐	PRE...	20	Enabled	Microsoft ...	Allow TC...	Out	Allow	TCP	*		*		%System... Domain
☐	PREC...	21	Enabled	Network ...	Allow UD...	Out	Allow	UDP	*		*	123	%System... Any
☐	PRE...	22	Disabled	Inbound 3...	Block ext...	In	Block	TCP	*	3389	*		Any

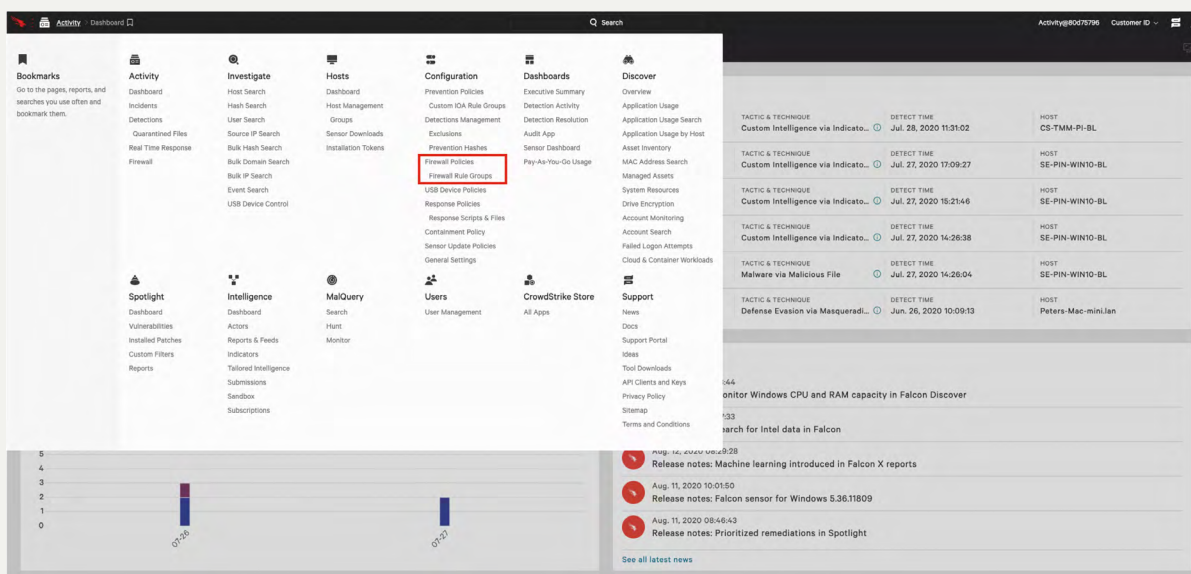
You can see that the changes haven't been saved, as indicated by the brown bar across the top of the page. Also, from this screen, you can edit the order of the firewall rules.

All Firewall Rule Groups Test Rule Group (Disabled)													
Unsaved changes on the rules tab													
RULES FIREWALL POLICIES AUDIT LOG													
Rule group details								Cancel	Save	Delete	Enable group		
NAME				DESCRIPTION						STATUS			
Test Rule Group										Disabled			
Selected 0 of 22								Enable		Disable	Delete		
								Edit precedence		Create new rule			

Before leaving the page, save any changes and click the Enable Group button.

CONFIGURING A FIREWALL POLICY

Back in the main menu, navigate to the Firewall Policies page.



The Firewall Policies page has a default policy and any other policies previously created. In the previous section, you created a rule group. In this step, you can either apply that rule group to an existing policy or add it to a new policy. To add the rule group to a new policy, click the Create New Policy button.

Firewall Policies							
WINDOWS POLICIES							
4 policies				Create new policy		Edit precedence	
PRECEDENCE 1	POLICY STATUS Enabled	POLICY NAME Domain Controller Policy	CREATED Feb. 11, 2020	LAST MODIFIED Feb. 11, 2020	APPLIED 0	PENDING 0	
PRECEDENCE 2	POLICY STATUS Enabled	POLICY NAME Laptop policy	CREATED Feb. 12, 2020	LAST MODIFIED May. 5, 2020	APPLIED 0	PENDING 0	
PRECEDENCE 3	POLICY STATUS Enabled	POLICY NAME Standard Remote Policy	CREATED Apr. 30, 2020	LAST MODIFIED Jun. 30, 2020	APPLIED 1	PENDING 0	
DEFAULT POLICY	POLICY STATUS Enabled	POLICY NAME Default (Windows)	CREATED Feb. 3, 2020	LAST MODIFIED Feb. 3, 2020	APPLIED 16	PENDING 0	

Give the new policy a name and optional description, and click “Next.”

Create new policy

×

PLATFORM

Windows

NAME (REQUIRED)

Temporary Test Policy

DESCRIPTION

CANCEL

NEXT

The next step allows you to build a new policy using existing policies for convenience or to build from an empty policy. Make your choice and click the Create Policy button to continue.

Create new policy

×

START WITH AN EMPTY POLICY OR COPY ALL RULE GROUPS FROM AN EXISTING POLICY

☐ Empty policy

☐ Existing policy

BACK

CREATE POLICY

After selecting the Create Policy button, you'll be directed to the Policy Settings page. There are three areas to this page. The top of the page includes four tabs: Settings, Assigned Host Groups, Assigned Rule Groups and Rule Summary. Also included in the top section of the page are the policy Enable and Delete buttons.

Configuration > Firewall Policies > Temporary Test Policy

Configuration@598956b4 Customer ID

All Policies Temporary Test Policy (Disabled)

SETTINGS ASSIGNED HOST GROUPS ASSIGNED RULE GROUPS RULES SUMMARY

Policy details Delete Enable

NAME	DESCRIPTION	PLATFORM	STATUS	PRECEDENCE
Temporary Test Policy		Windows	Disabled	4 of 4

Firewall policy settings Cancel Save

Enforcement and monitoring

Enforce policy ☐ Monitor mode ☐

Enforce this policy's rules and override the firewall settings on each assigned host. Disables native firewall rules. Override all block rules in this policy and turn on monitoring. Allows all traffic and shows block events as "would be blocked."

Default traffic rules

All firewall rules are applied in precedence order first. Remaining traffic uses these settings.

Inbound traffic

Allow or block all inbound traffic by default. Block All

Outbound traffic

Allow or block all outbound traffic by default. Allow All

The middle section of the page is the Enforcement and Monitoring section. Once the policy has been enabled and the "Enforce policy" option is toggled to the "on" position, the "Monitor mode" toggle will then be available to turn on as well. This gives you the opportunity to see the effect of the rules without blocking traffic.

Configuration > Firewall Policies > Temporary Test Policy

Configuration@598956b4 Customer ID

All Policies Temporary Test Policy (Enabled)

SETTINGS ASSIGNED HOST GROUPS ASSIGNED RULE GROUPS RULES SUMMARY

Policy details Delete Disable

NAME	DESCRIPTION	PLATFORM	STATUS	PRECEDENCE
Temporary Test Policy		Windows	Enabled	4 of 4

Firewall policy settings Cancel Save

Enforcement and monitoring

Enforce policy ☒ Monitor mode ☒

Enforce this policy's rules and override the firewall settings on each assigned host. Disables native firewall rules. Override all block rules in this policy and turn on monitoring. Allows all traffic and shows block events as "would be blocked."

Default traffic rules

All firewall rules are applied in precedence order first. Remaining traffic uses these settings.

Inbound traffic

Allow or block all inbound traffic by default. Block All

Outbound traffic

Allow or block all outbound traffic by default. Allow All

The last section on the page is the “Default traffic rules” section. Depending on the rules you’ve configured, you can then decide how all “other” traffic should be handled.

The default is to block all inbound traffic and allow all outbound traffic.

The screenshot displays the Falcon Firewall configuration interface for a policy named "Temporary Test Policy (Enabled)". The interface includes a top navigation bar with "Configuration", "Firewall Policies", and "Temporary Test Policy" breadcrumbs, a search bar, and user information. Below the navigation bar are tabs for "SETTINGS", "ASSIGNED HOST GROUPS", "ASSIGNED RULE GROUPS", and "RULES SUMMARY". The "SETTINGS" tab is active, showing sections for "Policy details", "Firewall policy settings", and "Enforcement and monitoring". The "Enforcement and monitoring" section includes a toggle for "Enforce policy" and a "Monitor mode" toggle. The "Default traffic rules" section is highlighted with a red border and contains the following content:

Default traffic rules

All firewall rules are applied in precedence order first. Remaining traffic uses these settings.

Inbound traffic

Allow or block all Inbound traffic by default.

Block All

Outbound traffic

Allow or block all outbound traffic by default.

Allow All

APPLYING FIREWALL RULE GROUP TO POLICY

Now that you have created a rule group and a new policy, you can assign your rule group to your new policy. On the Policy Details page, click on the Assigned Rule Groups tab.

The screenshot shows the 'Policy Details' page for 'Temporary Test Policy (Enabled)'. The 'ASSIGNED RULE GROUPS' tab is highlighted. The page includes sections for Policy details, Firewall policy settings, and Enforcement and monitoring. The 'Enforce policy' section has a toggle for 'Monitor mode'. The 'Default traffic rules' section shows 'Inbound traffic' and 'Outbound traffic' settings, both set to 'Block All' and 'Allow All' respectively.

The Assigned Rule Groups page allows you to assign multiple rule groups and edit the precedence. You can assign the Test rule group created earlier by clicking the Assign Rule Groups button.

The screenshot shows the 'Assigned Rule Groups' page for 'Temporary Test Policy (Enabled)'. The 'Assign rule groups' button is highlighted. The page includes a table with columns for Precedence, Status, Rule group name, Description, Rules, Last modified, Modified by, and Actions. A message at the bottom states 'No firewall rule groups assigned to this policy'.

The next window will include all of the rule groups previously created. This gives you the opportunity to create very specific rules without having to duplicate your effort. Select the rule group or groups you'd like to assign to this policy and click the Assign to Policy button.

Assign firewall rule group

	Status ▾	Rule group name ▴	Description ▾
☐	Enabled	Default Corporate	Base policy for all corporate endpo...
☐	Enabled	Domain Controller Rules	Rules specific to domain controllers
☐	Enabled	Remote systems	Rules for corporate laptops
☐	Disabled	Server Rule Group	Rules specific to servers
☒	Enabled	Test Rule Group	
☐	Enabled	Test Rules	Rules in test mode
☐	Enabled	Web Server Rules	Rules for web servers

Need to create a new firewall rule group? [Go to firewall rule groups](#)

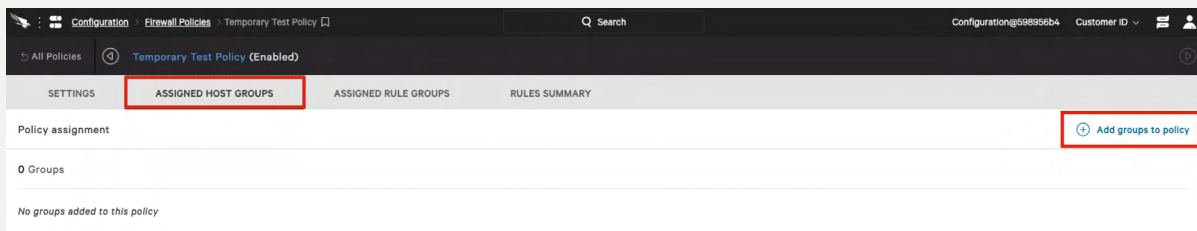
CANCEL
ASSIGN TO POLICY

Back on the Assigned Rule Groups page, your selected rule groups are displayed. The Rules Summary tab will display all of the rules from the multiple groups now included in the policy.

Configuration > Firewall Policies > Temporary Test Policy							
Search							
Configuration@598956b4 Customer ID							
All Policies Temporary Test Policy (Enabled)							
SETTINGS ASSIGNED HOST GROUPS ASSIGNED RULE GROUPS RULES SUMMARY							
Edit precedence Assign rule groups See all rule groups							
Precedence	Status	Rule group name	Description	Rules	Last modified	Modified by	Actions
PRECEDENCE 1	Enabled	Test Rule Group		21	Aug. 25, 2020 06:39:27	peter.ingebrigtsen@crowdstrike.com	

ASSIGNING A FIREWALL POLICY TO A HOST GROUP

For a firewall policy to be assigned to specific hosts, the firewall policy needs to be assigned to a host group. A host group is what it sounds like: a group of hosts that typically have a similar set of characteristics, such as operating system or type of user. In the firewall policies setting, there is a tab titled "Assigned Host Groups." You can see which host groups have been assigned to the specific rule group you're looking at. In this case we have yet to assign any host group. To assign this firewall policy to a Host group, you can pivot directly from the page using the Add Groups to Policy button.



You can select a host group directly from the new window by checking a box. Or, there is also an option to create a new group using the “Go to Groups page” link.

Add groups to policy

☐

NAME

DESCRIPTION

☐

Pre-Production Testing_...

Group created from Migrating Assignment Rule from Policy Pre-Production Testing

☒

NAME

DESCRIPTION

☒

Prevention

☐

NAME

DESCRIPTION

☐

RTR Group

☐

NAME

DESCRIPTION

☐

Server

Linux

☐

NAME

DESCRIPTION

☐

Servers

☐

NAME

DESCRIPTION

☐

SKO-SecOps-Demo

☐

NAME

DESCRIPTION

☐

ST Group

☐

NAME

DESCRIPTION

☐

Standard Linux

☐

NAME

DESCRIPTION

☐

Threat Hunting Dynamic

☐

NAME

DESCRIPTION

☐

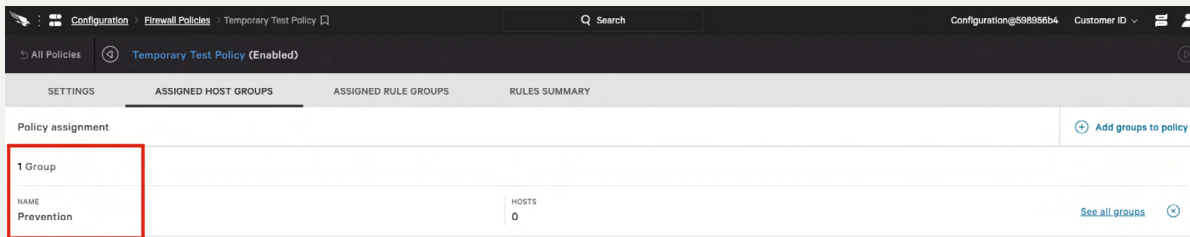
TMM Corp Demo

Need to create a new group? [Go to Groups page](#)

CANCEL

ADD GROUPS TO POLICY

After checking the box and clicking the Add Groups to Policy button, you are directed back to the Assigned Host Groups page where you see the host group has now been assigned your firewall policy.



Applying firewall rules to your environment can be an effective way to minimize the attack surface. However, there may also be unintended consequences to implementing firewall policies. To better understand firewall policies, please refer to [the documentation](#) in the Falcon console.

SUMMARY

Falcon Firewall Management makes it easy to manage host firewalls that are native to the operating system. With Falcon Firewall Management, you can simplify operations by using the same lightweight Falcon agent, management console and cloud-native architecture. A centralized approach with a single management console for both endpoint protection and host firewall management streamlines workflows and increases visibility across endpoint security controls.

ADDITIONAL RESOURCES

[Falcon Firewall Management User Guide](#)

[Falcon Firewall Management Demo Video](#)

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

