

SOLUTION BRIEF

Integrated Solution for Optimizing Security Orchestration with Automation

Executive Summary

As the digital attack surface expands, security teams must also expand their defense capabilities. With Fortinet and Rapid7, security teams can quickly respond to threats on the network by blocking hosts at the perimeter, isolating them on the internal network, and preventing lateral movement—all from their existing collaboration tools, such as Slack or Microsoft Teams.

Increasing security measures and tools for the expanding digital attack surface means more alerts for security teams to investigate and more context switching in the investigation process, among other issues. Everyday security practitioners spend an exorbitant amount of time jumping around the dozens of different tools within their tech stack just to gather the context they need to take action. This creates several challenges for security teams, including alert fatigue, a lack of qualified security personnel to manage new tools, and slower response times. This means they're often unable to respond to the threats they face quickly enough, being less effective in the way of prevention, and even increasing the time window for potential damage.

Joint Solution

Rapid7 and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. InsightConnect is a security orchestration and automation solution to enable teams to accelerate and streamline time-intensive processes with little to no code. With over 290 plugins, teams can easily connect tools and customize connect-and-go workflows, freeing up time to tackle other critical challenges. With significant time savings and productivity gains across overall security operations, security teams can go from overwhelmed to operating at maximum efficiency in no time.

The integration of Rapid7 InsightConnect and the Fortinet FortiGate next-generation firewall (NGFW) enables customers to take actionable responses of network threats to the next level through the power of automation. Hosts and networks can now be blocked in seconds, and through your company's existing communication channels, such as Microsoft Teams and Slack, can save your security team precious time and enable them to focus on what matters most.

Joint Solution Components

InsightConnect Plugin

The Fortinet FortiGate plugin connects the Fortinet firewall to the InsightConnect orchestration engine. It performs a number of address object management actions on the firewall and is the automation component for this solution. This plugin is used to build custom Fortinet workflow automation or leverage one of the [prebuilt workflow templates](#) that feature this plugin.

InsightConnect Workflows

Workflows are a sequence of steps and logic that replicate security processes. Rapid7's InsightConnect has a library of prebuilt workflow templates that can be imported with a single click.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Rapid7 InsightConnect

Joint Solution Benefits

- Equip security operations center (SOC) teams with the context for prompt and efficient response to threats
- Automated blocking of malicious hosts and networks to prevent lateral movement
- Block hosts and networks directly from Slack and Microsoft Teams in seconds and with visibility from your security team

FORTINET®

Fabric-Ready

Fortinet FortiGate Next-Generation Firewall

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate NGFWs are powered by artificial intelligence (AI)-driven FortiGuard Labs and deliver proactive threat protection.

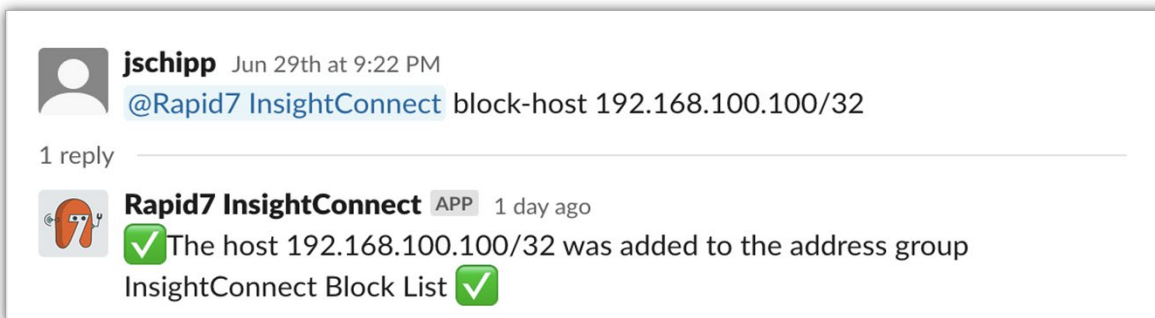
Joint Solution Integration

The Fortinet FortiGate plugin for InsightConnect allows users to automate common firewall management tasks, such as host and network blocking, unblocking, and checking if a host is blocked, through the management of address objects and groups. Security teams often have pre-established firewall rules and policies configured for their networks. This solution taps into an existing policy such as a “deny all” and manages the addresses in the group applied to that policy. In addition, the plugin features host and network whitelisting, as well as the option to disallow blocking of RFC1918 addresses, enhancing confidence and providing a safe way for security teams to block malicious hosts effectively.

By leveraging one of the Fortinet workflows for Slack or Microsoft Teams, users can begin blocking hosts from chat and collaboration tools.

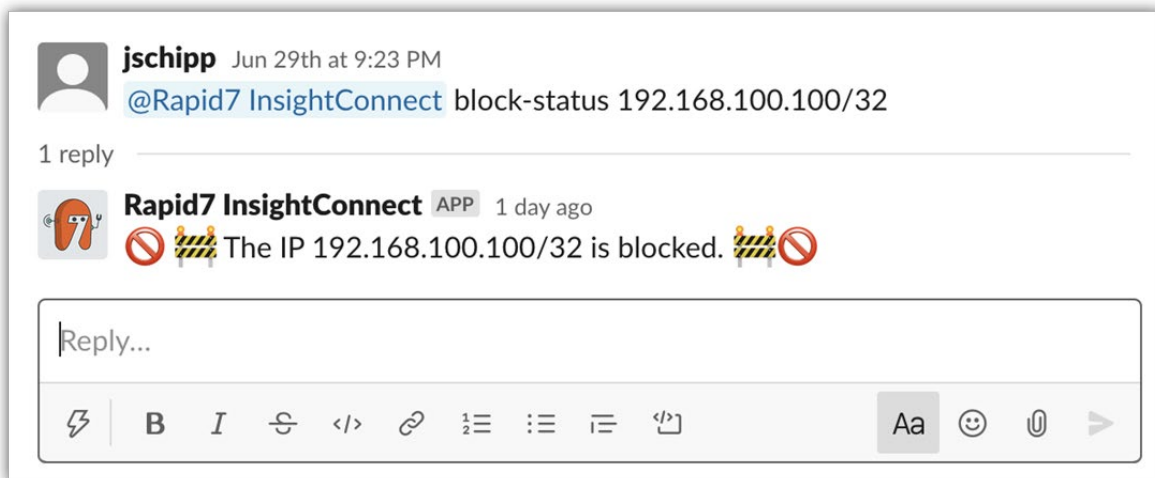
- https://extensions.rapid7.com/extension/Block_Host_with_Fortinet_Firewall_from_Microsoft_Teams
- https://extensions.rapid7.com/extension/Block_Host_with_Fortinet_Firewall_from_Microsoft_Teams
- https://extensions.rapid7.com/extension/Check_Host_Block_Status_with_Fortinet_Firewall_from_Microsoft_Teams
- https://extensions.rapid7.com/extension/Check_Host_Block_Status_with_Fortinet_Firewall_from_Slack

Slack Command to block a host



A screenshot of a Slack message. The sender is 'jschipp' with a profile picture of a person, dated 'Jun 29th at 9:22 PM'. The message content is '@Rapid7 InsightConnect block-host 192.168.100.100/32'. Below the message, it says '1 reply'. A reply from 'Rapid7 InsightConnect' (with an 'APP' badge and '1 day ago') shows a green checkmark icon and the text: 'The host 192.168.100.100/32 was added to the address group InsightConnect Block List' followed by another green checkmark icon.

Slack Command to check if a host is blocked



A screenshot of a Slack message. The sender is 'jschipp' with a profile picture of a person, dated 'Jun 29th at 9:23 PM'. The message content is '@Rapid7 InsightConnect block-status 192.168.100.100/32'. Below the message, it says '1 reply'. A reply from 'Rapid7 InsightConnect' (with an 'APP' badge and '1 day ago') shows a red circle with a diagonal line and a yellow and black hazard sign icon, followed by the text: 'The IP 192.168.100.100/32 is blocked.' Below the message is a text input field with the placeholder 'Reply...' and a rich text editor toolbar with icons for bold, italic, link, code, list, and text color.

Figure 1: Blocking and unblocking hosts can be done quickly and easily from Slack and Microsoft Teams using the prebuilt workflows (Slack illustration below).

Joint Use Cases

- **Block Host with Slack**—Blocks or unblocks a host or network with Fortinet firewall via Slack command and reports information back to Slack
- **Block Host with Microsoft Teams**—Blocks or unblocks a host or network with Fortinet firewall via Microsoft Teams command and reports information back to Teams

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 9,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our [website](#), check out [our blog](#), or follow us [on Twitter](#).



www.fortinet.com