PeerPaper Report

The Future of Firewalling: How a Platform Approach Can Lower Security Costs

Based on Real User Reviews of Cisco Solutions

2021

IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Organizations often struggle to achieve an effective security posture because of the complexity of managing disparate point security solutions that don't integrate well. The prevalence of remote workers and cloud apps has also eroded strict perimeters. A new generation of firewalls can address this challenge by providing application workload control and network control on premises, in the cloud, and at the Secure Access Service Edge (SASE) at the cloud edge. This paper takes on this topic, examining how platform-based controls and inspection points are able to the deliver lower costs and pervasive security modern organizations need. It is drawn from real user reviews of Cisco Secure Firewall and Secure Workload (Tetration) on IT Central Station.

CONTENTS

INTRODUCTION

Most organizations lack the time, money, and expertise required to knit together an effective security posture with multiple point security tools. The proliferation of encrypted traffic, remote workers, and cloud applications demands security control and inspection at more points than ever. Traditional network-based firewalling must be complimented by protection for application workloads and infrastructure. For application workloads, the security perimeter has to be extended to the workload itself — a new kind of firewall. This paper explores how users perceive the evolution of firewalling technology, and its role in today's security reality. It is based on real user reviews of Cisco Secure Firewalls and Cisco Secure Workload (Tetration) on IT Central Station.

Main Takeaways:

- Today's complexity often leads to errors and misconfigurations that leave organizations vulnerable.
- The network team must be able to keep pace with DevOps / DevSecOps demands for agility. Dynamic and automated policies between network and application workload-level firewalls are critical.
- Mitigating risks arising in this new landscape requires a new concept for firewalling—one that offers control, visibility, and tight endpoint and application integration on-premises, as well as in the cloud and at the cloud edge with an emerging Secure Access Service Edge (SASE) capability.
- Such a platform-based firewall of the future concept is actually available today. It lowers costs and produces measurable gains in security effectiveness.
- Organizations can radically enhance their security postures by embracing "firewalling," – the notion of tightly integrated control between the network and application workload layers.
- Success requires both flexibility and centralization. It means enabling segmentation and consistent, coordinated, and policy-driven control and inspection across physical and logical control points as well as across disparate networks and application workload environments.

The Evolving Security Landscape

It's well known that the security landscape has changed significantly in recent years. For security practitioners, the shifts have been especially dramatic. Networks are far more heterogeneous. As a result, achieving consistent policy management and enforcement is an acute challenge.

Maintaining unified visibility over networks, endpoints, and cloud assets has also become increasingly difficult. Today's complexity often leads to errors and misconfigurations that leave organizations vulnerable. The figure below illustrates a simplified view of this challenging environment. The red triangles represent the areas where a firewall must be actively monitoring and/or defending digital assets. The red data center area encompasses both firewalling at the application workload level as well as "east-west" traffic for major flows inside the data center.

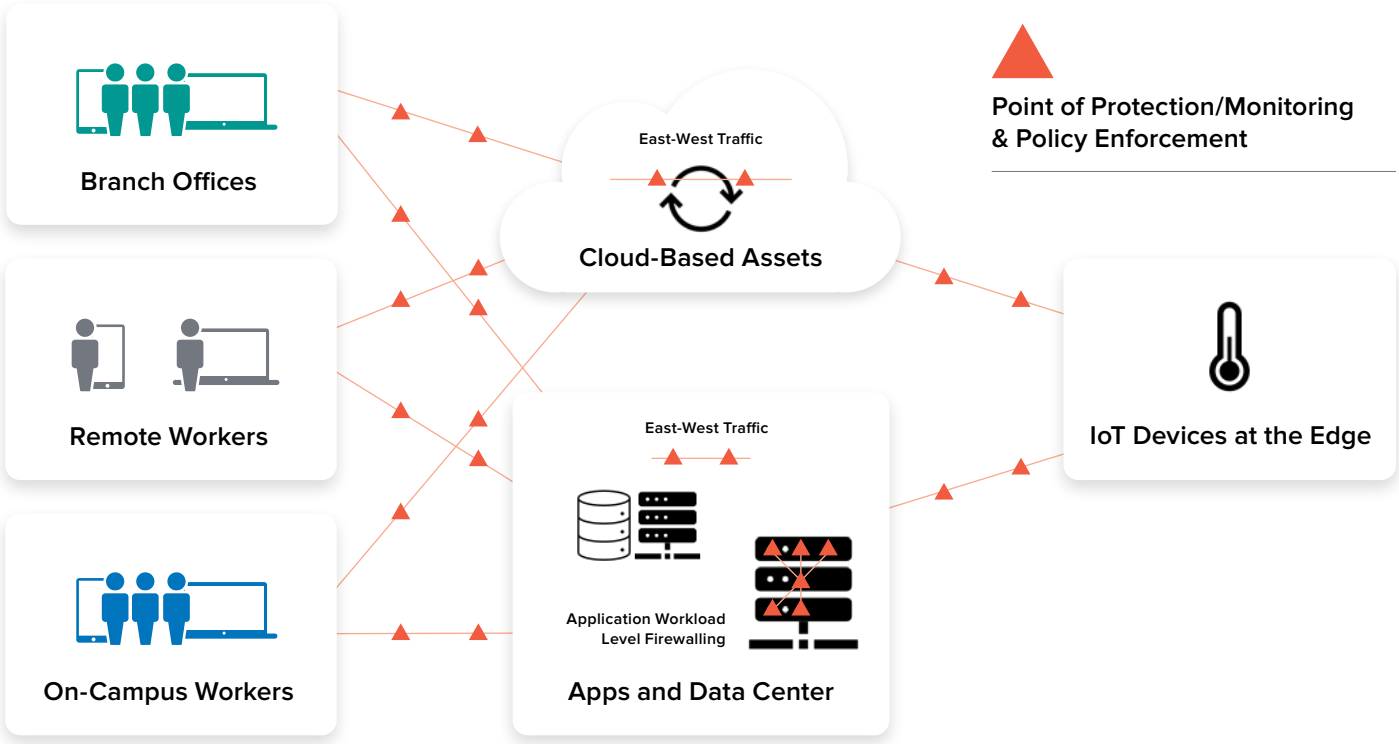
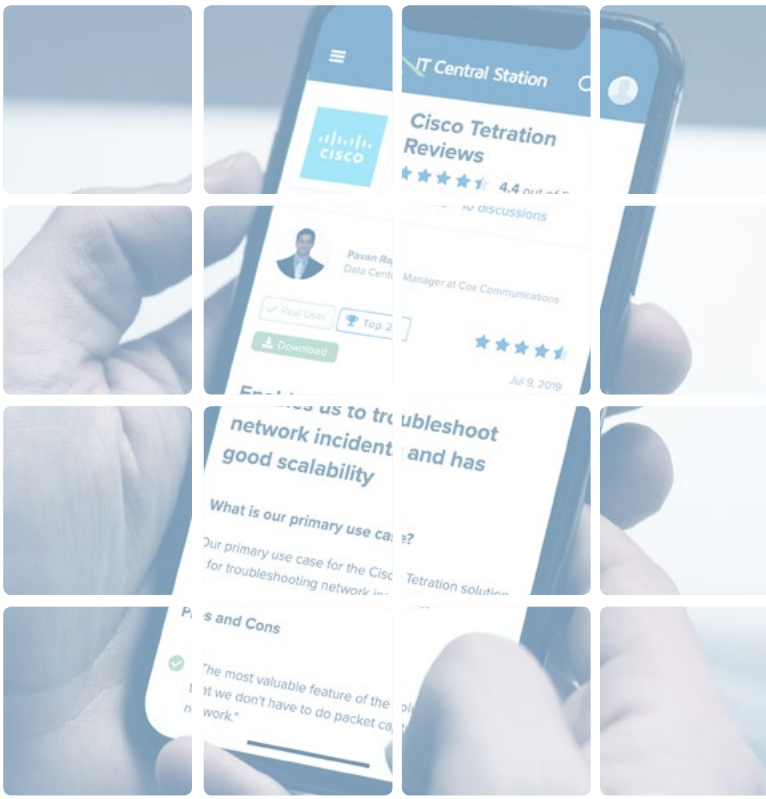


Figure 1 - A simplified view of today's firewalling challenges, where users, digital assets, and workloads must be monitored and defended across multiple, divergent networks and application infrastructure, including the cloud, on-premises and at the edge. This includes "east-west" traffic inside the data center and cloud infrastructure as well as "app-to-app" workload traffic inside various servers. The red triangles represent areas where control and segmentation are required.

The Future of Firewall Concept

As environments become more heterogeneous and spread out, the firewall ceases to be solely appliance-based, and instead becomes a function — tasked with coordinating endpoint and application controls for comprehensive protection in the data center, on premises, and in branch offices. Organizations regain control, reduce costs, and achieve consistent security policies, logging, and threat intelligence using an integrated platform-based solution. By embracing "firewalling" — with coordinated, policy-driven, control, and inspection across physical and logical control points among disparate networks and application workload environments — organizations dramatically enhance their security posture.



"We were using multiple products in the past. Now, we have it all centralized on one product.

What It Takes to Power the Firewall of the Future

Advanced firewalling must embody distinct capabilities if it is to provide a cost-effective platform approach that improves security posture. IT Central Station members have weighed in on the issue. From their perspective, the firewall of the future must offer a consistent policy model and policy management. The toolsets should blend flexibility with centralization and integrate threat intelligence into their core functionality. Monitoring and visibility into endpoints, threats, and application workloads are needed to help teams confidently protect their entire environments. As well, the platform must lend itself to SASE transformation.

Security Toolsets That Combine Flexibility and Centralization

Firewall users want a security toolset that combines flexibility and centralization:

- "A flexible and easy to manage solution for segregating our servers from the rest of the environment." - IT Specialist who uses AFA Firewall at a government agency

- "The flexibility to grant anyone access to the network easily and in a secure way is its most valuable feature." - Group Electrical Engineer Consultants who uses Cisco ISE at a communications service provider (Cisco ISE is an identity and access management solution that tightly integrates with Cisco Secure Firewall to deliver a zero trust model for the workplace and workforce.)

- "Our organization has been improved by the solution because we can be assured that the firewall is secure. It gives us more flexibility to monitor other things." - Senior Network Administrator who uses Cisco Secure Firewall at Washington Trust Bank, a financial services firm

Centralization complements flexibility in enabling firewall administrators to work efficiently. A Security Officer who uses Cisco Secure Firewall at a government agency remarked, "We were using multiple products in the past. Now, we have it all centralized on one product. We can do our content filtering and our firewall functions in the same place."

"This efficient, time-saving, centralized device manager is easy to deploy and requires minimal administrative IT resources," said an IT Manager who uses Cisco Defense Orchestrator at Egypt Foods group, a consumer goods company. A Product Consultant at a tech services company added to this insight, saying, "With Cisco Defense Orchestrator, we can manage the complete Cisco Security solution. It provides a simple and centralized way to manage all products." (Defense Orchestrator is the cloud-based management option for Secure Firewall.)

Monitoring and Awareness to Get a Better Handle on the Entire Environment

IT Central Station members stressed how sophisticated, holistic monitoring, coupled with detailed awareness, is critical to the impact made by a next generation firewall. To this point, granularity of monitoring was what mattered to a Security Officer who uses Cisco Malware Protection at a healthcare company. He related that "the visibility and insight this solution gives you into threats is pretty granular. It has constant monitoring." His team is able to get onto the device trajectory to look at a threat, but also see what happened prior to the threat. As he said, "You can see what other applications were incorporated into the execution of the threat."

> **"The visibility and insight this solution gives you into threats is pretty granular. It has constant monitoring.**

For example, he related, "You have the event, but you see that the event was launched by Google Chrome, which was launched by something else. Then, after the event, something else was launched by whatever the threat was. Therefore, it gives you great detail, a timeline, and continuity of events leading up to whatever the incident is, and then, after. This helps you understand and nail down what the threat is and how to fix it."

"The telemetry gives me the visibility on the particular path," said a Senior Manager of Cloud

Ops and Engineering who uses Cisco Secure Workload (Tetration) at a communications service provider with 10,000 employees. “It helps to analyze the whole fabric itself. I also get to know what condition we have and on which interfaces. We look at heavy traffic so we can share the particular load across to other interfaces as well.”

Consolidated Firewall Management

The ability to consolidate firewall management is also seen as an advantage when it comes to addressing the multi-faceted challenges of today’s complex security landscape. Users of next generation firewalls spoke to this point in their reviews. A Technical Team Lead Network & Security who uses Cisco AMP at Missing Piece BV, a tech services company, framed the issue by sharing: “With Cisco AMP, or any Cisco security products, you get Cisco Threat Response. Threat Response takes the intelligence from all your different solutions, then combines it with sources, like VirusTotal, and includes general information that Cisco has available on those threats.”

> **... it is very easy to go from what’s happening on my environment to what’s happening in the world.**

In his case, as he remarked, “If I see a file somewhere, I can with one click go from my console to Cisco Threat Response, and there it will be enriched, saying, ‘We have already seen this piece of software two months ago in Japan. This is what we thought of it. We did an automatic analysis on it. These are the indicators on this piece of software being either malicious or benign.’ With SecureX’s Threat Response, it is very easy to go from what’s happening on my environment to what’s happening in the world.”

The dashboard was important to a Senior Manager who uses Cisco Secure Firewall at HCL Technologies, a computer software company, in terms of the value of consolidating firewall management. He said, “We have a complete analytical view of the traffic behavior. We can immediately find anomalies.”

Segmentation with Points of Control

Firewalling, both at the network and application workload levels, is about enabling segmentation and introducing control points where they are required. In the case of a Sr. Regional Director at a small tech services company, Cisco Secure Workload (Tetration) enables automated micro-segmentation, which enables visibility into networks and additional security. He said, “This improves the entire organization by saving time, resisting attacks, and allocating resources properly.”

> **This improves the entire organization by saving time, resisting attacks, and allocating resources properly.**

A Solutions Architect at Liberty Global, a comms service provider with over 10,000 employees, said, “If your organization has a micro-segmentation strategy then this [Cisco Secure Workload] is a good solution. It works to improve visibility by creating connection metrics between applications and having the proper policy in place.” He found Cisco Secure Workload (Tetration) to be simple to implement, using micro-segmentation to secure endpoints.

In fact, his organization didn’t even bother looking at other vendors because they felt Cisco had the only solution on the market that covered micro-segmentation and application visibility. He

added, “It works to improve visibility by creating connection metrics between applications and having the proper policy in place.”

An IT Specialist who uses Cisco NGFW at a consultancy with over 1,000 employees also related that the primary use case for Cisco firewalls is to segment networks. As he put it, “We’re using them on the perimeter network for traffic filtering. Since deploying them, we have seen a maturing of the security in our organization.”

Consistent Policy Model and Policy Management

Consistency ranks high for firewall users when it comes to policy models and policy management. As a Technical Director who uses Cisco Secure Malware Protection (formerly AMP, which is available at the firewall and on endpoints) at Ridgewall Ltd, a wholesaler/distributor, explained, “The AMP and Cisco Umbrella combination has made life a lot more secure and enables us to deliver consistent policy. When people are in our building, we’ve got a reasonably consistent policy because we have greater control. But the minute a person leaves the building and connects via phone [hotspot] or at an Internet cafe, we lose most of the traditional protection we had. The endpoint becomes everything.”

> **Instead of taking three hours or two days, I could do it in 30 minutes.**

This platform approach has decreased Ridgewall’s time to detection, relative to where they were with previous products. The customer added, “Before this type of next-gen solution, we were relying on things like antivirus, which is pretty poor and didn’t produce much in the way of protection, certainly around ransomware and other things. We were relying heavily on perimeter protection, like firewalls. That was, of course, completely ineffective when people took their laptops home.” For a Systems Architect at a university, Cisco’s cloud-based Defense Orchestrator (CDO) firewall manager makes it easier to ensure that policies are consistent and “that there aren’t too many mistakes being made through a more manual process.”

> **Automated policy application and enforcement saves significant time when adding devices, users, or new locations.**

Policy automation saves time and enhances enforcement. “Instead of logging into several devices, one at a time, I could push the policy at one time and mitigate, let’s say, a vulnerability,” said a Systems Engineer who uses Defense Orchestrator at a tech services company. “Instead of taking three hours or two days, I could do it in 30 minutes.” On a related note, the firewall of the future streamlines security integrations. As the CTO of Secure Networkers, a tech services company, put it, “Defense Orchestrator brings everything together.”

A manager who uses Cisco Secure Firewall at BTC, a communications service provider, noted that “Automated policy application and enforcement saves significant time when adding devices, users, or new locations. Our clients use automated policy application and enforcement.” He offered the example of this process reducing implementation time in a large deployment scenario, and with a bank that needed to deploy to additional branches. He added, “When you add more users or you add more devices, when

you create a profile of the policies, they will be available in a matter of minutes, regardless of the number of branches or users or applications. It reduces the time involved in that by 75 percent."

Concern about "shadow" firewall rules (i.e., rules that are not operative because they are behind other firewall rules) figured into the assessment offered by a Network and Data Center Platform Manager who uses Defense Orchestrator at a manufacturing company. He shared, "It's helped us identify where we've got shadow rules and duplicated objects which aren't being used. Where before, we probably wouldn't have detected those objects and the shadow rules - where there's a rule that conflicts with another rule, we wouldn't necessarily have picked that up. Now, CDO highlights that for us. It makes us have a more consistent rule set. It makes our configuration better because we haven't got rules in there that are not doing anything or are duplicated." Another benefit of this automated clean-up of firewall rules is that it increases firewall performance and helps to keep networks operating at peak performance.

Integrated Threat Intelligence

The integration of threat intelligence, especially when paired with automation, leads to gains in security effectiveness and productivity. As a CIO who uses Cisco Malware Protection (AMP) at Per Mar Security Services, a security firm, explained, the integration of Cisco SecureX's Threat Response feature with products including Cisco Email Security, Cisco Secure Firewall, Secure Analytics (Stealthwatch), Threat Grid, Umbrella and third-party solutions drives improvements in overall threat awareness. He shared, "Talos is out there as the guiding force, applying visibility from around the globe, and the insights that it gains, and then feeds back into all the security platforms. Threat Grid lets us see and track hashes with the forensics that we get. It is just

> "This solution interfaces with Talos Intelligence, Threat Grid, Threat Response, and SecureX.

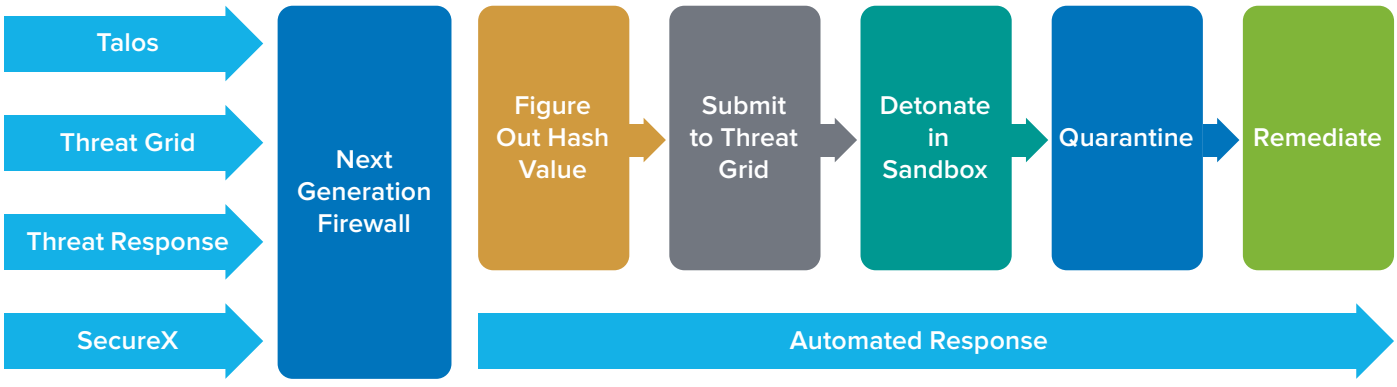


Figure 2 - Threat intel integration, leading to an automated threat remediation workflow in a next generation firewall.

out-of-bounds crazy what we're able to do in a very short period of time."

"This solution interfaces with Talos Intelligence, Threat Grid, Threat Response, and SecureX. All of these things are integrating together and a lot of stuff is now starting to happen automatically," said the healthcare Security Officer. For example, he shared, "if a threat is detected, it is automatically interfacing with Talos Intelligence to figure out what that threat is and the hash value of whatever file that is. If it thinks it's suspicious, it automatically submits it to Threat Grid, which detonates the file in the sandbox, but also in the cloud, and returns a report saying whether the file, or whatever it is, is an actual threat/incident." From there, the solution is able to remediate and quarantine the threat. "You find out about it later," he added. "It's doing a lot of stuff in the background as the integration with other tools increases." Figure 2 depicts this architecture and workflow.

Further to the point of automation and threat integration working synergistically, a Network Security Consultant who uses AFA Firewall at a consultancy, related the following possible

> **If your company encounters one type of malware, once, it is automatically updated in your environment.**

scenario. "If your company encounters one type of malware, once, it is automatically updated in your environment. And when it is updated, Talos then updates every firewall in the world, so even if those other firewalls have not yet encountered those particular types of malware, because Talos automatically updates everything, they're able to block those types of malware as well. Talos is very beneficial."

CONCLUSION

Given the difficulties organizations are having building effective security postures out of point solutions, it is fortunate that a new generation of firewall tools can help close the gap. The firewall of the future offers a much-needed solution to dealing with diverse endpoints and infrastructure that can be running almost anywhere. They comprise a firewall platform with broad functionality and strong but flexible integrations of key security features. With centralized management and monitoring, they facilitate a cost-lowering approach to security.

The firewall of the future is the ultimate solution for a world where firewalls have ceased to be a thing, but instead operate as a function. They enable organizations to regain control and achieve consistency. The technology achieves this aim by using an integrated, policy-driven method that strategically coordinates advanced security protections throughout heterogenous networks, hitting multiple logical control points in the process.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT CISCO SECURITY

Cisco Secure Firewall and Secure Workload enable coordinated segmentation at the network and application workload levels. They include the Cisco SecureX platform that unifies visibility and automates workflows. We enable SecOps, NetOps, DevOps, and ITOps teams to efficiently coordinate, enhancing enterprise security posture. As well, Cisco delivers cloud-based and on-prem firewall management options.

All Cisco Secure solutions benefit from the Cisco Talos threat research organization. Talos insights power the threat intelligence used across the Cisco Secure platform, enabling greater security visibility and efficiency. We enable organizations to share context around incidents, accelerating investigations and incident management by aggregating and correlating global intelligence and local context in one view. And our orchestration drag-drop canvas allows custom workflows with no/low code, eliminating friction while automating routine tasks.