The Future of the Firewall

Achieving a stronger posture today while building a bridge to meet tomorrow's business and security demands

Table of Contents

Abstract

The purpose of this white paper is to discuss the evolution of network security and what it will take to protect an organization's environment for the future.

As networks become more heterogeneous, it becomes increasingly difficult for organizations to achieve consistent policy management and enforcement and maintain unified visibility. The complexity of these interconnected networks often leads to errors or misconfigurations, leaving them vulnerable to ever-evolving, sophisticated threats.

What can an organization do to regain control and achieve consistency? It starts with an integrated approach to security that places the firewall front and center.

Firewalls are still the cornerstone of an organization's network security strategy, but just as networks have evolved, so too must our firewalls. In the past, the firewall was a single appliance at the ingress/egress "perimeter" acting as a policy-driven control point to permit or deny network traffic. To succeed in today's digital world, organizations need to think beyond single firewalls and embrace "firewalling"— a policy-driven method for strategically coordinating advanced security protections across logical control points throughout heterogenous networks.

"Firewalls are still the cornerstone of an organization's network security strategy, but just as networks have evolved, so too must our firewalls."

Firewalling will be a critical step for organizations to better align security with changing business and networking needs. Cisco has been hard at work building an integrated security platform with our firewall at the foundation to enable businesses to make the transition.

With firewalling, organizations that are digitally transforming can achieve a stronger security posture today while building a bridge to meet tomorrow's business and security demands.

Section 1: The history of the firewall

The evolution of network security

Traditionally, the firewall was placed as a gatekeeper on the network edge. It acted as an all-encompassing control point, inspecting network traffic as it traveled across this perimeter. Sitting at the network's ingress/egress point, the firewall was responsible for validating communications: internal network traffic was considered inherently trustworthy, and external traffic was considered inherently untrustworthy. Rule sets and policies were created and enforced at this single point of control to ensure that desired traffic was allowed into and out of the network and undesirable traffic was prevented.

Comparing the network perimeter to a moat around a castle, the firewall acted as a drawbridge controlling all traffic in and out of the fortress.

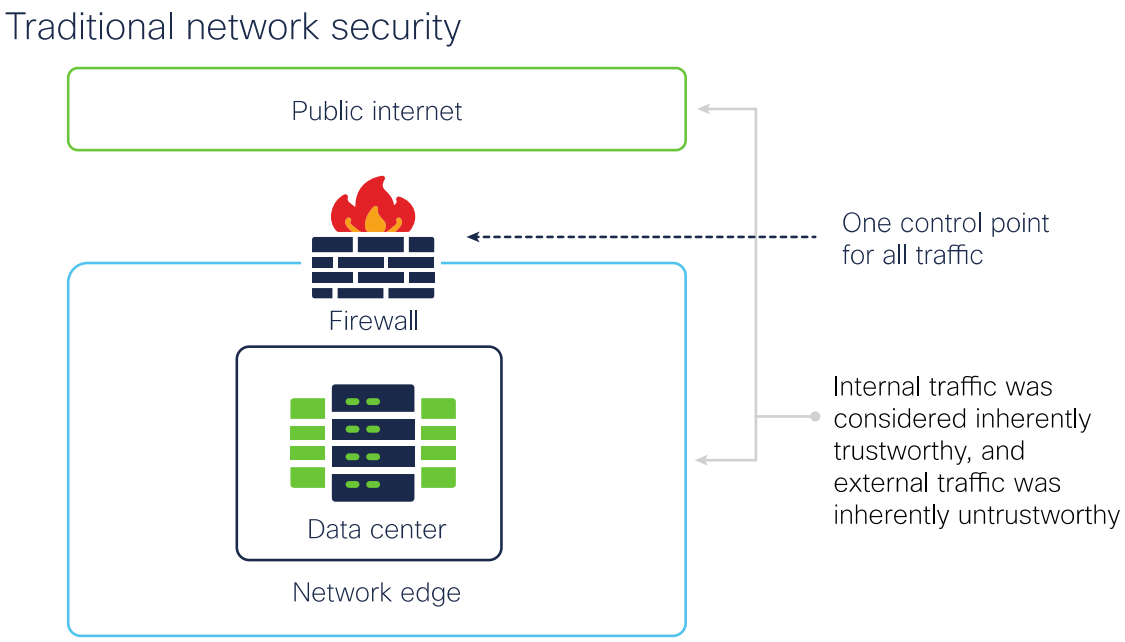

Figure 1. Traditional network firewall approach

Along came the cloud. And apps.

It wasn't long before this practice of enforcing security through a single control point was challenged. First, there was the rise of remote access and enterprise mobility. But transformation really kicked in with cloud computing. When business moved to the cloud, devices and users began migrating en masse outside of the controlled internal network, which made the single control point model ineffective. Soon, there were multiple perimeters. They all needed to be secured. There was no effective way to put one moat around the network.

Today, branch office locations, remote employees, and increasing use of cloud services are driving more data away from the traditional "perimeter," bypassing the traditional security control point completely. Additionally, many businesses have adopted a bring your own device (BYOD) model, allowing employees to access sensitive business applications through their private computers or mobile devices. In fact, more than 67% of employees use their own devices at work - an upward trend with no end in sight . Mobile

devices and laptops connected via publicly accessible Wi-Fi networks are prevalent, even crucial for day-to-day business operations.

Further, the overwhelming majority of business locations and users also require direct access to the Internet where an increasing majority of cloud-based critical applications and data now live. Businesses continue to deploy workloads across multiple cloud services, operating systems, hardware appliances, databases, and more. Applications and data become further de-centralized, and networks subsequently become more diverse.

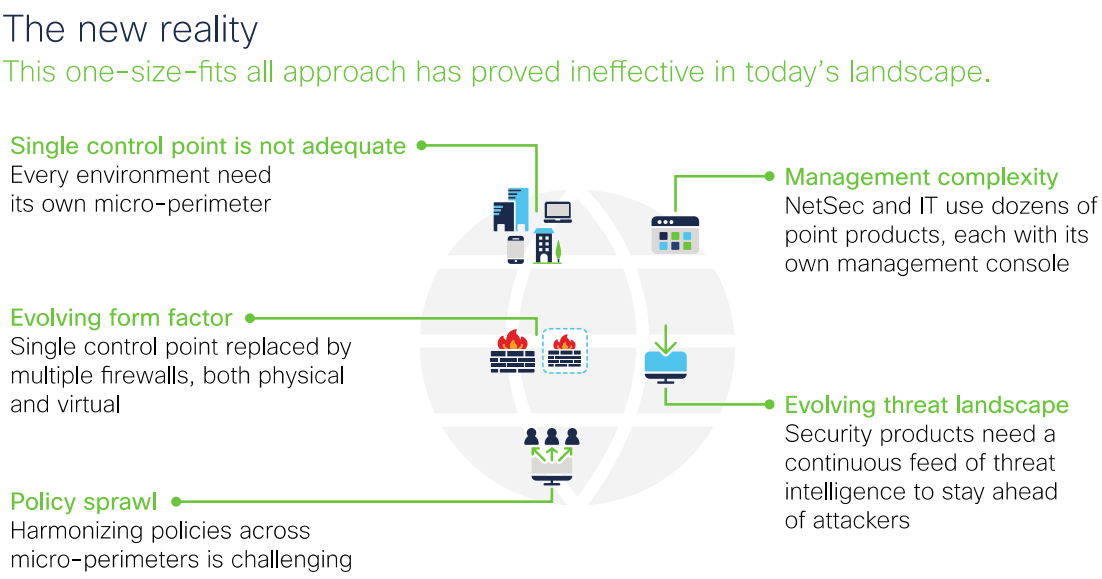

Figure 2. Network complexity and evolving threats are challenging the traditional firewall model

A new, more complex reality

While these innovations allow for a more interconnected and productive work environment, they've changed the very nature of the way we do business. The days of controlling applications and authorizing users on-premises have morphed into dynamic, multicloud ecosystems delivering services and applications across enterprises. Not only that, we're also managing business-critical third-party relationships. Vast expansion and outsourcing provide economies of scale and efficiency, but not without tradeoffs. This evolution of network architectures has greatly increased our attack surfaces and made the job of protecting business networks, data, and users strikingly more complicated.

Fighting back with point products

Typically, organizations have attempted to address these challenges by adding the "best" point security solution to address each new problem as it emerged. Because of this approach, we have seen tremendous device "sprawl," with the average enterprise using up to 75 security tools[1]. Multiple security products across different vendors can pose significant management problems for network security teams.

[1] "Defense in depth: Stop spending, start consolidating," CSO, March 4, 2016.

[2] "Navigating Network Security Complexity," ESG Research Insights Report, June 2019.

[3] "Navigating Network Security Complexity," ESG Research Insights Report, June 2019.

In most cases, a proliferation of security devices and capabilities leads to an increase in the risk of attack. When asked, 94% of IT and infosec professionals were concerned that increased network complexity makes them more vulnerable, and 88% want to make network security policy changes more agile[2].

Between January and July of 2019, 3,800 data breaches were disclosed – a 54% surge over the first half of 2018[3]. This steep climb is a testament to the progressively sophisticated methods bad actors are using to breach networks. The growing rate of successful breaches is also an indication that traditional methods of network security are no longer standing up against modern threats.

More threats, more noise, even more risk

As malicious parties attack new vectors – from email to unvetted endpoints under BYOD policies, to web portals, and IoT devices, organizations are also driven to try any number of other approaches to protect themselves.

As discussed above, the trend of adding point products doesn't improve an organization's overall security posture. Quite the opposite. It creates more "noise" for security teams to manage. While they struggle to keep their eyes peeled for inevitable new attacks and malware seeking to exploit any vulnerability (either known or unknown), this added complexity makes the job of creating, managing, and enforcing security policies ever more difficult.

In response, network security teams are tasked with configuring multitudes of cloud resources individually, further increasing the chance of a security misconfiguration that could lead to a breach. A security control that's not implemented or implemented with errors can be the biggest culprit of all: 64% of organizations say that human error was the leading cause of a misconfiguration[4]. Whether such a mistake leads to a violation of compliance, an outage, or opens the door to an adversary, it's risk you can't afford.

It's time to rethink the firewall

Network security has become a daunting task. Today's personnel can't go on attempting to manage a mass assortment of point security solutions, cloud resources, and appliances. It's time for a different approach.

It's time for the firewall to take its place as the foundation for an agile and integrated network security platform that will lead to the for businesses of today and tomorrow.

Section 2: From firewall to firewalling

Why firewalling?

As our networks evolve to accommodate new ways of doing business, so too must our network security. In the current world of distributed IT assets, the firewall is still central to a robust security posture.

However, firewall requirements have increased significantly to protect the wide array of network infrastructures, connected devices, and operating systems from advanced threats. Consequently, our "traditional" firewall devices are being augmented by a mixture of physical and virtual appliances—some are embedded into the network while others are delivered as a service, are host-based, or are included within public cloud environments. Some are even taking on new form factors, such as clustered appliances that scale to large traffic requirements, software that runs on personal devices, SD-WAN routers, and secure Internet gateways. The activity of sharing threat intelligence across all these disparate firewall devices, regardless of their location, is vital for uniform threat visibility and a strong security posture.

To make the full shift and better secure today's networks, businesses must move away from the traditional "perimeter" approach. Instead they've got to establish strategic enforcement points across the entire network fabric, closer to the information or applications that need to be protected. Specifically, the creation of micro-perimeters at both physical and logical points of control has become a necessary reality.

We need to think less about the firewall as a standalone physical network device and more about the functionality of *firewalling*.

What is firewalling?

Make no mistake: the firewall is more relevant than ever. In fact, to secure today's networks we need **more** firewalls **everywhere**. The difference is that firewalling focuses on **how** you can establish policy-based controls everywhere:

Firewalling can provide an agile and integrated approach for centralizing policies, advanced security functionality, and consistent enforcement across your increasingly complex, heterogeneous networks. It should deliver comprehensive protections, visibility, policy harmonization, and stronger user and device authentication. Firewalling should also benefit from the sharing of threat intelligence across all control points to establish uniform threat visibility and control—dramatically cutting the time and effort needed to detect, investigate, and remediate threats.

In this way, firewalling becomes a key strategy for securing your complex network today. And provides a bridge to the future as your business—and the threat landscape—continues to evolve.

What is Firewalling?

Enforcement points are everywhere across today's heterogeneous networks.

Firewalling is delivering consistent threat prevention functionality with consistent policy and threat visibility so you can prevent, detect, and stop attacks faster and more accurately, everywhere.

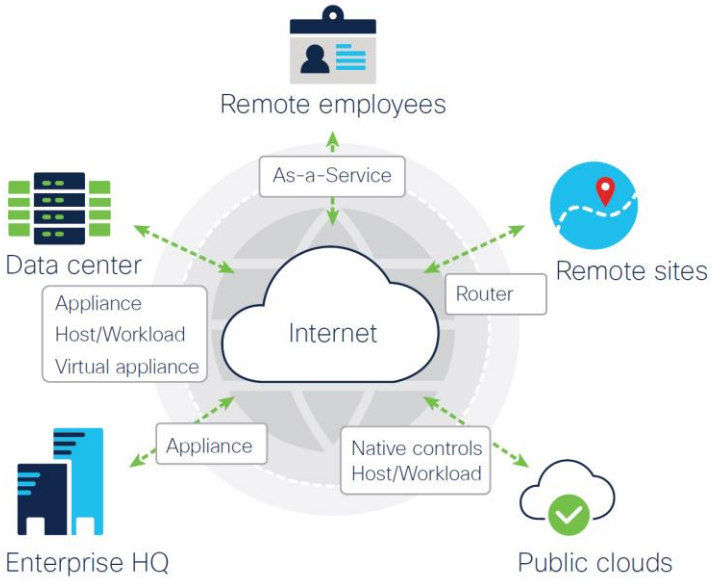

Figure 3. The core tenants of firewalling as a means to address the security challenges of modern networks

What does it look like?

Whether protecting assets and data in the cloud, on premises, or at a remote location, firewalling needs to consistently provide advanced threat protections, policy enforcement, and shared threat intelligence. The challenge is delivering that consistency across disparate environments where different devices are deployed and utilized.

Security breaches can originate from any device that has access to the Internet, regardless of whether it's in the corporate headquarters, data center, remote sites, public clouds, or any location where an employee is working remotely. That's why it's more important than ever to incorporate a robust set of security control points in more logical locations to reduce exposure and mitigate risks. Security controls are applied where needed on owned environments (physical or virtual appliances and network devices like routers) as well as non-owned environments (Security as a Service [SECaaS]), native controls, and workloads.

Extending security controls

Under the premise of a traditional firewall, since all internal traffic and authorized users were inherently trustworthy (and external traffic wasn't), protecting the entire organization was accomplished at the network perimeter. This network perimeter became the logical security control point to protect the entire organization. All network traffic, whether originating from the headquarters, a data center, or remote worker, was funneled through this single control point.

Of course, this model does not work in today's complex environments where an organization's IT infrastructure spans a wide variety of form factors and delivery models, including physical and virtual appliances, network- embedded routers or switches, delivered as-a-service, host-based, or included with a public cloud.

With a firewalling approach, consistent security controls are deployed to provide full visibility, unified policy, and comprehensive threat visibility. These security controls enable stronger user and device authentication across increasingly heterogenous environments. They gather, share, and respond to context about users, locations, devices, and more to ensure devices meet defined security requirements. Using consistent security controls at every micro-perimeter, security teams can start to automate tasks (such as auto-quarantine out-of-compliance users and devices, block questionable domains across all security controls, and support effective microsegmentation). In firewalling, full visibility provides a holistic view of all security alerts and indicators of compromise, and shared threat intelligence delivers the most up-to-date threat detection to any connected device.

Cloud-based management

And it's not just point products. The explosion of network perimeters and cloud resources has increased exposure for breaches as well. Safeguarding a business's most valuable assets in complex cloud environments while managing various security products is no small task. Security teams need instant visibility and streamlined management to help reduce misconfiguration.

Firewalling promotes a stronger security posture by supporting centralized, cloud-based management to help security teams cut through complexity and align policies throughout the organization. Templates can improve policy design and consistency by writing a policy once and scaling its enforcement across tens of thousands ofsecurity controls throughout a network. The use of standard policy templates to rapidly deploy new devices helps reduce configuration errors. As organizations grow, new deployments automatically inherit the latest policies. A scalable policy management system integrates multiple security features into a single access policy and optimizes policies across security devices to identify inconsistencies and quickly correct them.

What's more, a centralized, cloud-based management solution takes a team's capabilities to the next level. They can quickly identify risks across all devices, bringing them to a more consistent and secure state. With a single management console, objects can be compared across all devices to uncover inconsistencies and optimize the current security posture. Personnel can streamline policy management, improve efficiency, and achieve more consistent security while reducing complexity.

Fighting back with threat intelligence

As the network perimeter expands and the number of devices directly connected to the Internet proliferates, our attack surfaces also expand. Cybersecurity threats involving malware, cryptocurrency, phishing, and botnet activity are escalating, and cybercriminals are turning to machine learning and AI to exploit existing software vulnerabilities and expedite malicious attacks. Very few organizations have adequate resources to fully test and qualify all software vendor vulnerability patches – most are challenged to fend off the onslaught of emerging and evolving threats.

Another compelling aspect of firewalling can help here. Leveraging industry-leading threat intelligence with the latest threat research – some on a nearly up-to-the-minute basis – with access to protection updates helps mitigate the constant stream of threats. Threat researchers rapidly identify indicators of compromise and confirm and share threats quickly. Using economies of scale, they aim to protect organizations against developing threats before they happen. Sharing threat intelligence across interconnected networks, endpoints, workloads and cloud environments helps security teams correlate seemingly disconnected events, eliminate noise, and stop threats faster.

Firewalling begins and ends with the firewall as the cornerstone to future-proof network security

At Cisco, we've been hard at work bringing this vision into reality. We work with businesses and enterprises of all sizes across the globe, and all of them need their network security to be more agile and more integrated – baked into the network itself. That's why we're delivering the most secure architecture ever, a powerful and comprehensive platform with the firewall as the foundation.

Providing an unprecedented level of protection through this concept is a major component of our security strategy. The Cisco security portfolio and Cisco's family of firewalls keep you one step ahead of evolving threats with world-class security controls everywhere you need them, consistent policy and visibility, and innovations that improve security operations.

In an era where the threat landscape is more dynamic than ever before, Cisco brings networking leadership and cutting-edge technology together so you can have the strongest security posture available today and tomorrow.

What are the risks of not firewalling?

As networking has advanced, organizations have adapted, deploying various point products to support business requirements and operations. They've done the same as new attack vectors are publicized, adding product after product to protect against the latest XYZ threat. Those that rely on a traditional firewall to secure every connected device across multiple perimeters risk exposing their most valuable data and assets to security breaches. According to the 2019 Cybersecurity Almanac, cybercrime damages will cost the world $6 trillion annually by 2021[5].

These threats can infiltrate a network quickly and jeopardize the operations of a business that lacks comprehensive network security and endpoint visibility.

That said, securing an organization's network, cloud environments, devices, and data wherever they are is a huge burden on security teams. Traditional firewalls provide a limited view; IT needs greater visibility across the entire network with shared threat intelligence to detect and block threats earlier and faster. Firewalling goes further by delivering a comprehensive security posture based on unified management and comprehensive security capabilities such as intrusion prevention, URL filtering, and advanced malware protection leveraging automation and machine learning for efficiency.

Without a firewalling strategy in place, network complexity can lead to misconfigurations, escalating the risk for a security breach. According to a Gartner report, "through 2022, at least 95% of cloud security failures will be the customer's fault."[6] By embracing a firewalling strategy of harmonizing security policies across multiple control points, organizations improve their overall security posture.

Section 3: Four steps for setting up your firewalling strategy

Step 1: Set the foundation for your successful firewalling strategy with a modern next-generation firewall. The right Cisco Secure Firewall will deliver consistent security policies, visibility, and improved threat response for your integrated security solution.

Step 2: Once you've selected your Cisco Secure Firewall, the next step is to standardize on a management solution. Consider these factors when determining which solution is right for your organization:

- Determine the preferred management location (on-premises, or cloud) and which group will be responsible for managing security (SecOps or NetOps).
- Most importantly, ensure the management solution aligns with IT's current and future goals. If you're moving workloads to the cloud, launching a vendor portal, or tackling digital transformation projects or SaaS applications you may want to adopt cloud-based management. If your organization relies on monolithic legacy applications, on-premise applications may suit your needs. Generally, legacy applications take some re-factoring to run properly on the cloud, and if there are no immediate plans to upgrade these applications, an on-premises management system is usually best.
- A cloud-based management solution helps network operations teams align policies throughout the organization, reduce complexity, and manage all security control points from a central dashboard. It simplifies orchestrating and managing policies consistently from one spot to protect against the latest threats. With a centralized, cloud-based application, you can streamline security management, deploy new devices faster with templates, and track all changes over time across your environment.

Step 3: Strengthen your security posture with integration. Your firewalling strategy should provide comprehensive coverage across all microperimeters and deliver protection and control across all connected devices and security solutions. Integrating security throughout your heterogeneous network, across cloud apps and services, corporate email, and all connected endpoints safeguards your business against the expanding threat landscape.

This step sets up your security team to block more threats, respond faster to advanced threats, and deliver automation across the network, to cloud apps, and endpoints.

Step 4: Finally, make sure your firewalling strategy incorporates ongoing advanced threat analysis to protect your business assets and help you stay ahead of new emerging threats. One of the easiest ways is to choose a solution that automatically provides the latest threat information to your network through your firewall. Up- to-date intelligence and full visibility enable security teams to understand the latest vulnerabilities. And if a threat makes its way inside, you can identify where and how it happened. Built-in

next-generation IPS functionality automates risk rankings and impact flags to identify priorities so the most critical assets and information can be identified and prioritized. Security teams can immediately take corrective action and remediate threats, staying focused on the most critical assets versus being overwhelmed by the "noise," making SOC operations more secure.

It starts with the right firewall as the foundation

Today's security teams need:

Better security backed by industry-leading threat intelligence to protect your complex network and detect threats earlier and act faster.

A way to **efficiently set, scale, and harmonize security policies** across your network.

Visibility and reduced complexity with unified management and automation to accelerate security operations and improve their experience.

Networking and security that works together to maximize your existing investments. The right solution will provide a deep set of integrations for comprehensive security that protects everything, everywhere.

The benefits of a firewalling strategy with Cisco Secure Firewall

Turn your entire network into an extension of your security architecture: By sharing common policy, intrusion prevention capabilities, and other core functions with Cisco Secure Firewall, switches and routers can perform security enforcement, tying the network infrastructure into a comprehensive security portfolio. Share threat intelligence across your architecture quickly to correlate seemingly disconnected events, eliminate noise, and stop threats faster.

World-class security controls: Cisco Secure Firewall provides superior threat efficacy to protect your complex network against today's increasingly sophisticated attacks. Industry-leading, advanced threat intelligence helps your organization find new malware domains and malicious URLs as well as unknown or undisclosed vulnerabilities to detect threats earlier and act faster. Built-in, next-generation IPS delivers comprehensive visibility with automated risk rankings and impact flags to identify priorities for your security team, minimizing noise. Retrospective security keeps you informed and continually analyzes threats after initial detection to better identify sophisticated malware that may initially hide from detection.

Unified policy and threat visibility: Security teams can achieve policy consistency and harmonization by standardizing and pushing security controls across every device -– from network appliances to hosts and across the cloud. Cisco's flexible and centralized management lets your team apply scalable controls to many devices quickly and easily to maintain consistent policies. Reduce complexity with unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP. Streamline security policy and device management across extended networks and accelerate key security operations such as detection, investigation, and remediation.

Section 4: A future-ready security solution

The way we work has changed. Our businesses and networks have transformed, changing the rules of network security. These developments require us to re-think the firewall and embrace firewalling.

Cisco is driving innovation to address these trends with a security platform that delivers world-class security controls everywhere you need them with consistent security policies and visibility, backed by industry-leading threat intelligence. The latest generation of Cisco Secure Firewall forms the foundation of our portfolio of tightly integrated products.

Cisco's flagship cloud management solution – **Cisco Defense Orchestrator** – delivers policy harmonization across a variety of Cisco security products.

Included in every Cisco security product is **SecureX threat response**, an automated threat response solution that reacts to new cyberattacks by automatically sharing and deploying countermeasures across the entire security architecture.

Secure Endpoint delivers global threat intelligence, advanced sandboxing, and real- time malware blocking. AMP continuously analyzes file activity across your extended network for quick detection, containment, and removal of advanced malware.

Talos Threat Intelligence is a world-renowned team of full-time threat researchers, data scientists, and engineers who collect information about existing and developing threats. Talos underpins the entire Cisco security ecosystem and delivers protection against attacks and malware. Talos provides visibility into the latest global threats, actionable intelligence on defense and mitigation, and collective response to actively protect all Cisco customers.

SNORT Next-Generation Intrusion Prevention System (SNORT NGIPS) is an industry-leading, open-source NGIPS that performs traffic analysis, packet sniffing/logging, and protocol analysis. SNORT NGIPS leverages Talos threat intelligence to help the entire security community by sharing policies that protect against developing threats.

Adaptable, trusted access everywhere based on context is available with Identity Services Engine (ISE). It provides intelligent, integrated protection through intent-based policy and compliance solutions.

Secure Access by Duo provides multi-factor authentication, endpoint visibility, adaptive authentication and policy enforcement with remote access and single sign-on to proactively secure access to applications.

Secure Network Analytics, Secure Workload, and Application Centric Infrastructure (ACI) work together, keeping tabs on your users wherever they go and their application workloads wherever they're located, using machine- learning, behavioral modeling, network infrastructure telemetry, and segmentation to outsmart emerging threats.

Implement your future-ready firewalling strategy by investing in the Cisco security platform and Cisco Secure Firewall. You'll gain the strongest security posture available today and be ready for tomorrow.

Section 5: Start building your future of the firewall today

Cisco brings networking leadership and cutting-edge security technology together to deliver the most secure architecture ever. Whether it's enhancing your network security by optimizing existing investments or transforming your routers into a firewall, Cisco continues to innovate.

Cisco Secure Firewall is network security designed for your digitally transforming business – from the company that built the network.

Learn more about Cisco Secure Firewall and get started on your future of firewalling today. And read more about the latest trends shaping tomorrow's networks in the 2020 Global Networking Trends Report.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA Cxx-xxxxxx-xx 01/20