Data sheet
Cisco public

Security Cloud Control

Contents

Organizations face a critical challenge today: Attackers are exploiting the weakest links in their networks, such as unsecured users, devices, and workloads. This threat landscape is complicated by the shift from traditional data centers to a distributed environment, where protecting dispersed data across multiple touchpoints becomes complex.

To address these threats, many organizations resort to using multiple security tools, leading to siloed teams, tech stacks, and management systems that hinder effective security. This fragmented approach results in unnecessary costs, longer deployment times, inconsistent security, and critical gaps.

Without a centralized platform, gaining a holistic view of security is challenging. Manual identification of misconfigurations is error-prone and can lead to breaches. There is a lack of skills, time, and resources to fully utilize security features and maximize ROI. Resolving access or policy issues is lengthy due to diverse security products. Admins spend excessive time crafting similar policies across different platforms. Operational issues are often addressed reactively, leading to downtime and suboptimal performance. Non-actionable alerts and overwhelming data cause analysis paralysis and hinder decision-making, with a missing sense of urgency.

A unified security platform aims to alleviate these issues by providing a comprehensive view of the security landscape, enabling consistent policy enforcement, simplifying troubleshooting, and offering actionable insights with the help of AI.

To meet the unique needs of various organizations and support diverse network firewall configurations, the focus is on three core objectives: simplifying operations, enhancing security, and improving clarity. We aim to streamline security management processes, strengthen defenses with advanced Zero Trust and vulnerability protection, and offer clear, actionable insights through AI-driven intelligence.

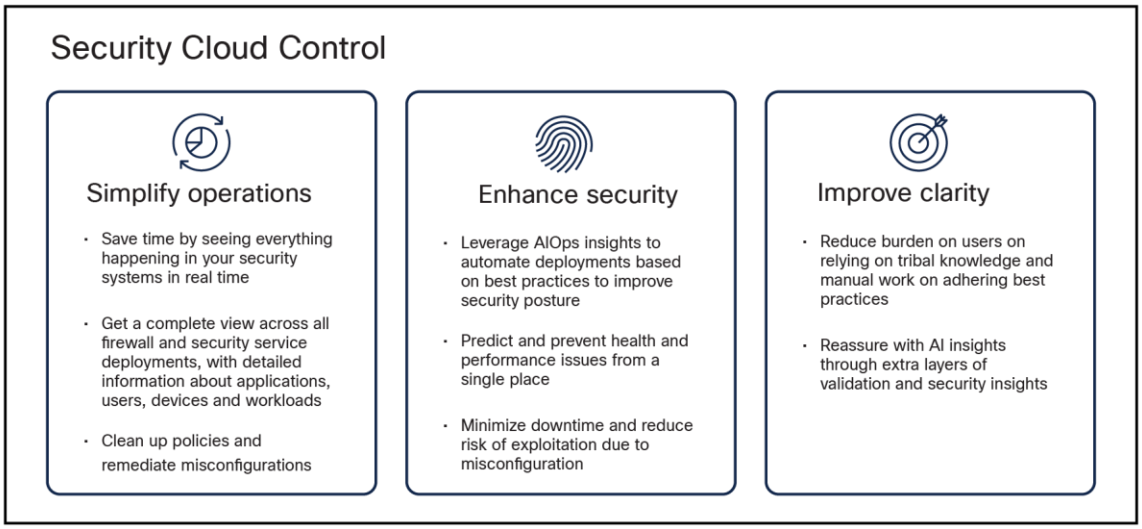

Figure 1.
Security Cloud control design principles - simple, efficient, and effective management.

Security Cloud Control

Security Cloud Control is a new, AI-native management solution to unify the security cloud, proactively surface actionable insights and automate resolution across hybrid environments. It is a modern micro-app architecture with consistent UI experience, common services, and a data bus that connects the configuration, logs, and alerts across the security cloud. AI is baked in from the start, going beyond AI assistants to proactively optimize policy, configuration, and to find and troubleshoot issues. It is designed to help teams get the most of out their Cisco Security investment—saving time and benefiting from simpler and streamlined policies.

Security Cloud Control allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Security Cloud Control centrally manages elements of policy and configuration across:

- Cisco Multicloud Defense
- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Meraki™ MX
- Cisco IOS devices
- AWS security groups

Security Cloud Control also incorporates the cloud-delivered version of Firewall Management Center (FMC), providing a fully unified experience between on-premises and cloud-based firewall management. This expands management of policy and configuration to Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual.

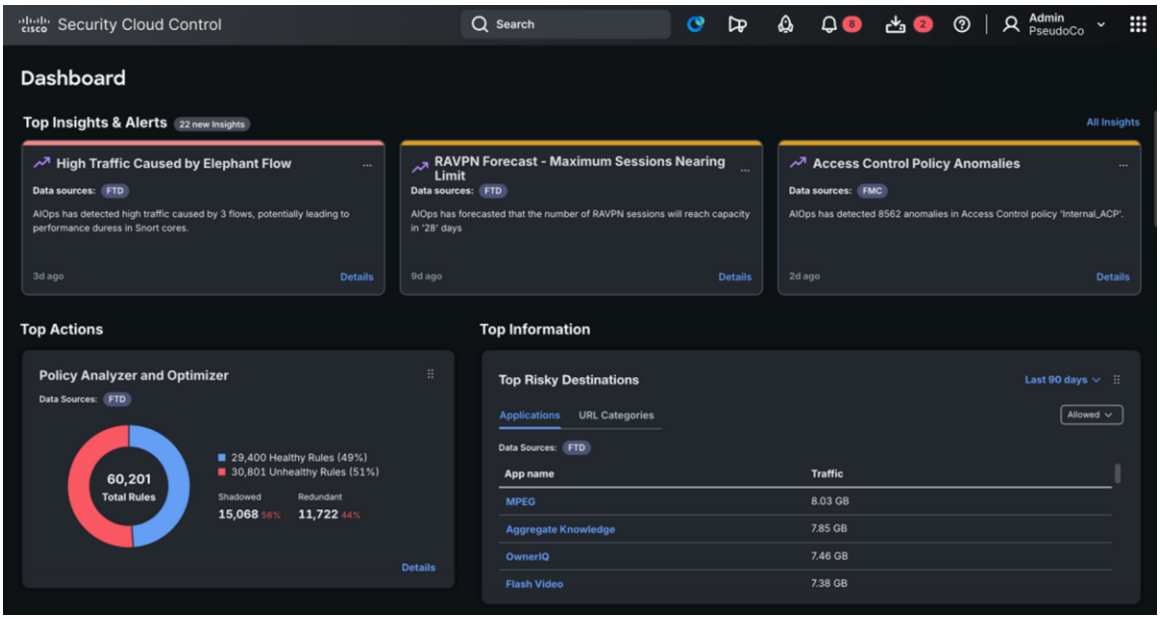

Figure 2.
Unified Dashboard - A Comprehensive view of firewall and security services

Setup is easy, fast, and frictionless, allowing customers to onboard and start managing hundreds of devices within hours. The intuitive user interface and focus on simplicity means that training requirements are minimal, with a learning curve measured in hours rather than days.

Flexibility and scale are attributes of our open API as well as being a cloud technology. Because it's a cloud-based solution, Security Cloud Control does not require capital expenditures, rack space, or manual patching and upgrading, dramatically reducing your operational costs.

It doesn't matter whether your organization has 5 or 5000 security devices. Security Cloud Control provides network operations teams with the ability to reduce time spent managing and maintaining security devices, enabling them to focus on what is most important to your core mission.

We are further simplifying the operations for our admins with the Firewall AI Assistant. It revolutionizes network security by tackling the complexity of firewall rule management.

Unified dashboard that enables our customers to gain a real-time, holistic perspective of their entire network and cloud security ecosystem. Customers can efficiently manage tens of thousands of security devices, coordinating multiple tenants under a centralized global administrator.

The level of visibility and management from Security Cloud Control helps on delivering the outcomes. From taking intent-based policies in one place and translating them throughout all the control points in your network to streamlining, troubleshooting and recommending policies that span multiple solutions, Cisco Security Cloud Control helps with it all.

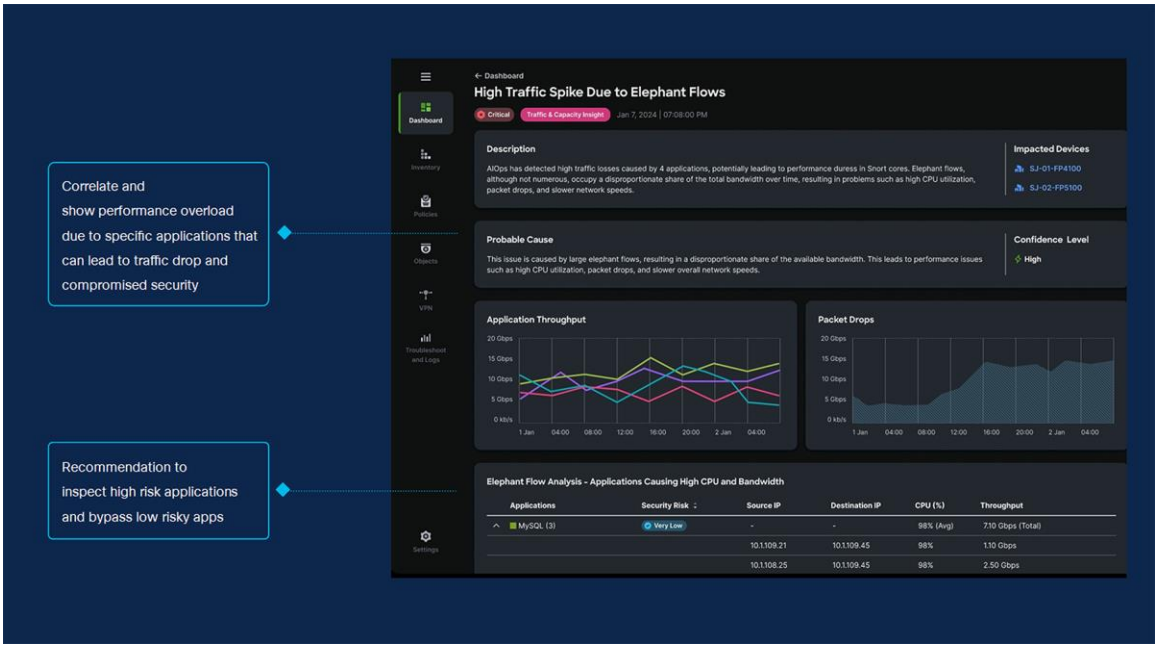

Figure 3.
Predictive insights with AIOps

Security Cloud Control benefits

Security Cloud Control simplifies network security management through centralized visibility, streamlined policy deployment, and real-time monitoring. It enhances operational efficiency by harmonizing security policies across multiple devices, ensuring consistent protection and rapid response to threats.

- **Simplify management**: Streamline security policy and device management across your extended network.
- **Critical Security Insights:** Our unified dashboard brings to light crucial security gaps in your network. It identifies misconfigured policies that could lead to breaches and provides actionable steps to fix them. It detects risky applications and URLs, ensuring you're utilizing all the security features you've purchased. It highlights vulnerable assets that need protection and logs all administrative changes across different products in one centralized location. Additionally, it prioritizes critical alerts to ensure they are addressed as top insights.
- **Proactive, Not Reactive:** Traditionally, we've flooded you with alerts, leaving you to figure out how to mitigate issues. Now, we're shifting to a proactive approach. Using AI, we predict when your system might hit its max capacity, identify the apps causing problems, and offer solutions to avoid downtime.
- **Simplified Operations with AI:** AI Assistant helps you understand policies and detect anomalies in your deployment. It can identify problematic rules, suggest necessary actions, and even write rules for you. This ensures consistent policy enforcement across your network.
- **Write Once, Apply Everywhere:** You only need to create network objects (like malicious IPs or URLs) once. These can be shared across different security products, ensuring comprehensive protection across your entire network.

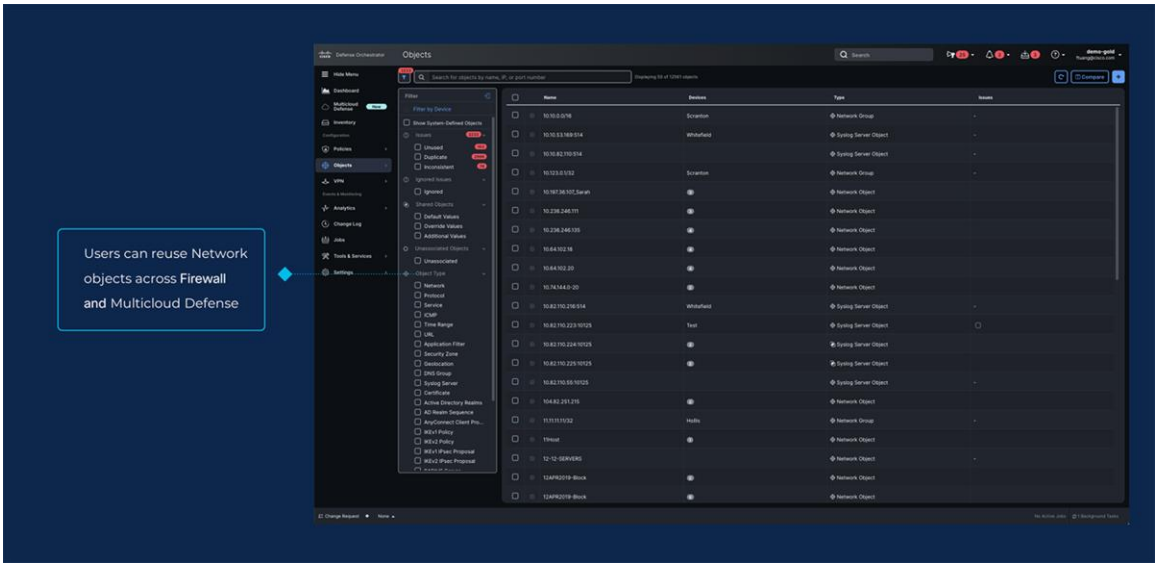

Figure 4.
Consistent Policy Enforcement - Sharing Network Objects across on-prem and Cloud environments

Security Cloud Control features

Security Cloud Control strengthens your security posture by aligning policies throughout your organization. Our solution addresses the challenge of staying on top of your policies when adding security tools. This is especially helpful for organizations with geographically dispersed locations as well as hybrid network environments.

The solution eliminates the time-consuming complexity of managing policies across distributed security devices. It helps prevent inconsistencies and gaps in your security.

You can manage from anywhere with a highly secure, always available, highly reliable, and scalable multitenant cloud solution. It frees up capacity for other priorities by strengthening and maintaining security posture in less time and with fewer resources.

Simplify operations and strengthen security using AIOps: AIOps provides predictive insights and automation to empower administrators simplifying operation, enhance security posture, boost operational efficiency and reduce costs.

Eliminate misconfigurations and optimize rules for simplified operations: The Policy Analyzer and Optimizer detects duplicate, redundant, shadowed, expired, overlapping, and mergeable rules. Apart from spotting anomalies, it delivers accurate implementation recommendations. You can download a change log and report from this service to keep your policy optimized.

Management of hybrid environments (ASA, FTD and Multicloud Defense): Streamlined workflow and integration between cloud security and on-premises/data center firewalls, you can now share objects and create VPN tunnels between Cisco Firewalls and Multicloud Defense. Static object sharing enables consistent policy outcomes across hybrid environments, eliminating administrative overhead and reducing potential for misconfiguration. Site-to-cloud VPN tunnels allow assets deployed across hybrid environments to communicate with one another via a secure connection.

Optimization for your existing platforms: Upon onboarding, Security Cloud Control will immediately be able to identify and flag common issues across firewalls that have been in production for years. After assessing and identifying all risks, you will now be able to swiftly remediate issues across all devices in bulk – bringing your devices to a consistent and more secure state. Security Cloud Control helps to correct the following issues:

- **Unused objects** are objects that will never be hit and cause issues during troubleshooting as well as add to potentially unwanted questions during audits.
- **Duplicate objects** are often found on a device and associate different names to the same IPs. Removing duplicate objects can improve the overall performance of the appliance.
- **Inconsistent objects** are objects that get represented differently across deployed firewalls. This is typically the most important object issue from a security perspective. For example, if you had an object name “block list” and all devices are supposed to have this object with matching variables or IPs, Security Cloud Control will quickly validate this. If the object is not consistent across firewall devices, Security Cloud Control will alert you and allow you to resolve the issue in seconds.
- **Shadow rules** are rules that will never be hit due to preceding rules that supersede them.

ASA-to-FTD migration: It is now easier than ever to migrate your environment from ASA to Cisco Threat Defense (FTD), thanks to Security Cloud Control’s embedded migration wizard. Manage both ASA and FTD from a single UI, enabling you to transition to NGFW in your own timeline!

Templates for consistent policy design: Using Security Cloud Control, you can now create, apply, and manage a consistent policy design across disparate devices from a single place. Our template feature allows you to create a "gold configuration" that can be replicated and customized. Once you are done, you can export and apply your standardized configuration to any new platform.

Simplified firewall OS upgrades: Often one of the most time-consuming and frustrating challenges that our customers face is maintaining the firewall OS for both features and vulnerabilities. Using Security Cloud Control, you can reduce the time it takes to perform Cisco ASA or Cisco Threat Defense (FTD) image upgrades by up to 90 percent. We take the guesswork out of planning and enable you to perform the upgrade in bulk across all your devices at once.

CLI in bulk: In addition to an intuitive web-based UI, we also provide our Command-Line Interface (CLI) users with a streamlined user experience as well. Security Cloud Control's CLI Tool gives users the ability to perform CLI commands in bulk across many devices at once, including the ability to create user-defined macros or shortcuts for your most common commands.

Audit of changes with change log: Customers can track changes through our change log to review what change was made, when, and who performed the change. All changes made in both the Security Cloud Control UI and the CLI Tool are captured.

Remote-access VPN monitoring and management: Visibility across remote user sessions and head-end devices with a historical view over 90 days for capacity planning. Extend visibility of user traffic by leveraging Cisco Security Analytics and Logging.

Cloud-delivered version of Firewall Management Center: Offers the same look -and feel as on-premises and virtual versions of Firewall Management Center, with:

- **Comprehensive visibility and policy control:** Provides exceptional visibility into what is running in your network and cloud so you can see what needs to be protected. Using this visibility, you can create and manage firewall rules and control thousands of web and custom applications used in your environment.
- **Automated security for dynamic defense:** Continually monitors how your network is changing, streamlining operations, and improving your security so you can focus on the threats that matter.

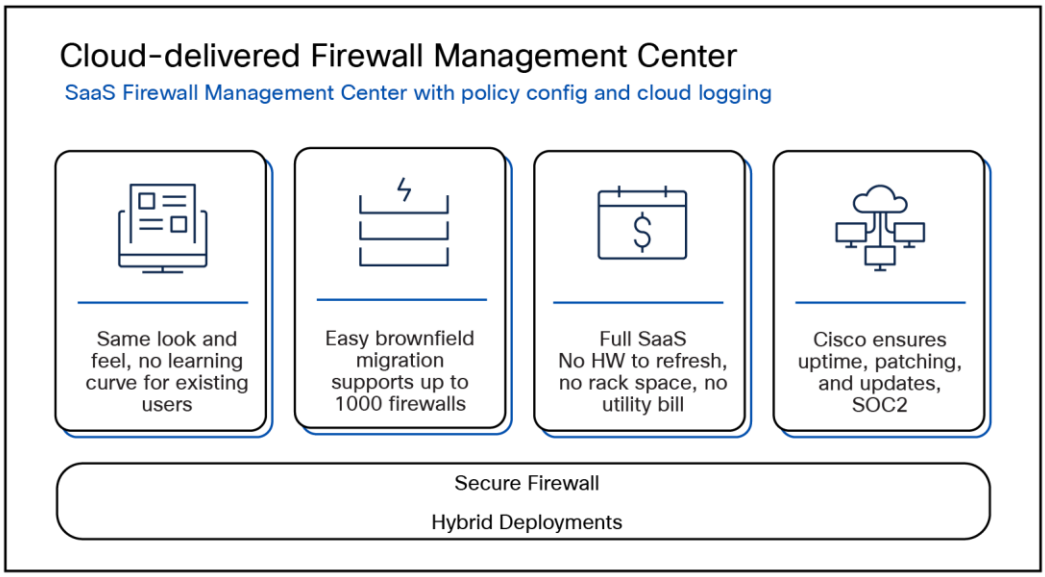

Figure 5.
Benefits of cloud-delivered Firewall Management Center via Security cloud control.

For more information, visit the Cisco Secure Firewall Management Center (formerly Firepower Management Center) Data Sheet.

For more information on Multicloud Defense, visit Cisco Multicloud Defense.

Table 1. Features and benefits

Objective	How we can make it happen
Fast deployment and device onboarding	• Security Cloud Control accounts are assigned in 24 hours, and you can start onboarding devices almost immediately. Devices can be onboarded as just a configuration, single device, or thousands of devices through bulk imports with no associated downtime. • Low-touch provisioning streamlines large-scale remote deployments. Available for Firepower 1000/2000/3000 Series running FTD version 7.0.3 and later (excluding 7.1).
AI Ops - Traffic and Capacity Insights	• Traffic and Capacity Insights offer both real-time and historical analyses of network traffic, aiding in the identification and resolution of problems and forecasting potential problems. • Allow Network security administrators to optimize resources, reduce mean time to resolution with risk-based prioritization, and align with best practice recommendations.
AI Assistant for Firewall – Rule creation and analysis	• Customers can ask the AI Assistant to explain the intent of the policies and assist with creating rule. • Simplifies the operations for our admins with the Firewall AI Assistant.
Policy Insights with Policy Analyzer and Optimizer	• In-depth review and enhancement of firewall policies, pinpointing and rectifying redundancies, duplications, overlapping, shadowed, and mergeable rules, as well as those that are expired or inactive. By providing tailored remediation recommendations, it ensures that firewall policies remain streamlined and efficient, significantly cutting down on deployment time.
Unified dashboard - A Comprehensive view of firewall and security services	• To gain a real-time, holistic perspective of their entire network and cloud security ecosystem. Customers can efficiently manage tens of thousands of security devices, coordinating multiple tenants under a centralized global administrator.
Object and policy analysis for optimization of existing devices	• At onboarding, Security Cloud Control will uncover areas for optimization and put the user in a position to quickly remediate the problems found. Common issues include duplicate, unused, and inconsistent objects across devices. We can also identify hit rates and shadow rules that will never be hit.
Options for proactive configuration and policy changes	• Security Cloud Control gives you options for how you can manage your devices centrally. If you prefer, you can deploy directly to the device immediately using the CLI Tool, enabling the use of “bulk” deployments, macros, and/or shortcuts for your most common commands. Next, you can also use the UI to provide a simple way to “stage” changes in the cloud during normal business hours and then push these changes out at your next maintenance window.
Security templates	• Leveraging an existing “gold configuration,” you can design and manage templates for easy, consistent deployment of your new devices.
Global search	• Allows you to quickly locate and navigate to devices managed by Security Cloud Control. It scans all the devices and objects in the system and displays them with indexing. With event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.
ASA-to-FTD migration	• Migrate your environment from ASA to Cisco Threat Defense (FTD) using Security Cloud Control’s embedded migration wizard.
Change log	• Track changes to the configuration being made within Security Cloud Control for accountability, auditing, and troubleshooting purposes.
Out-of-band notifications	• Changes made via ASDM or CLI (SSH) will be identified by the Security Cloud Control administrator as an Out-Of-Band (OOB) change. The administrator can make the decision to keep this change or revert back to the original configuration.
Backup and rollback of configurations	• Security Cloud Control backs up the configuration after every change and offers the ability to roll back to previous configurations.

Objective	How we can make it happen
Simple image upgrades	• Streamline the approach to performing OS upgrades for faster access to the latest patches and features.
Troubleshooting of potential issues	• Built into Security Cloud Control is the ability to pull live logs and run PacketTracer to help with troubleshooting of your devices.
Simple search	• See how policies are enforced across device types by searching for any object name, Access Control List (ACL) name, network, or application policy element.

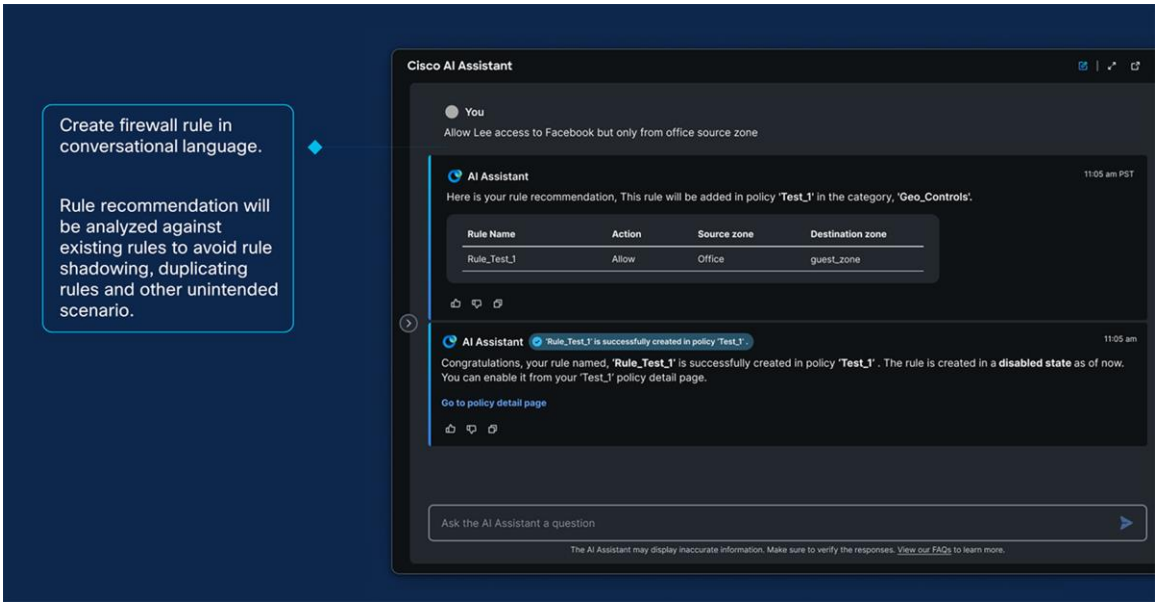

Figure 6.
AI Assistant for Firewall Rule Creation

Security Analytics and Logging (SAL) SaaS Overview

A cloud-delivered, Software-as-a-Service (SaaS) offering with a cloud-native data store, referred to as SAL (SaaS)

SAL (SaaS) is a full-feature offering providing cloud-based and cloud-delivered log management for Next-Generation Firewalls (NGFWs) running Cisco Firepower® Threat Defense (FTD) software, as well as devices running the Adaptive Security Appliance (ASA) software, independent of their management platform. SAL (SaaS) enables event viewing via APIs in Security Cloud Control (CDO) for firewall event logs.

Cisco Security Logging and Troubleshooting: Allows organizations to store firewall logs in the cloud and present visually in Security Cloud Control's event viewer. Correlate historical and/or live events from your firewall platforms for troubleshooting.

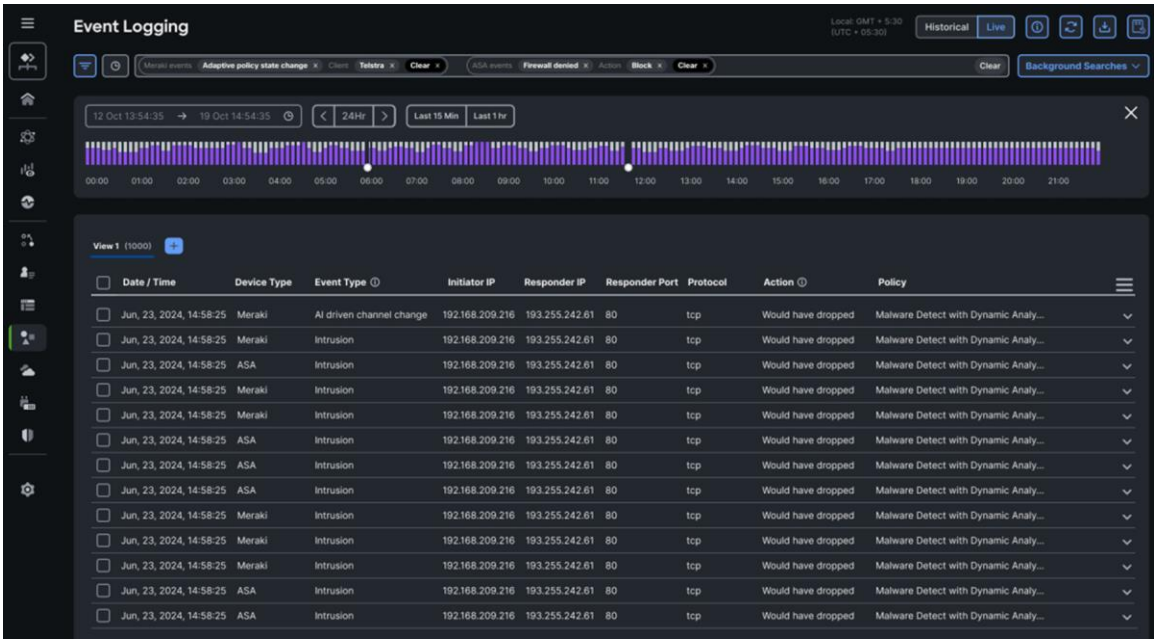

Figure 7.
Integrated cloud-based live logging to extend troubleshooting capabilities and provide historical visibility for audit purposes.

Required components and setup to run Cisco Security Analytics and Logging (SaaS):

Secure Event Connector: To capture Firewall Event Logs from cloud deployments, a Secure Event Connector (SEC) is needed. The SEC is a containerized application that can be installed on an on-premises or cloud Secure Device Connector (SDC), or even be set up to run in standalone mode. It receives events from Firepower Threat Defense (FTD) devices and Adaptive Security Appliance (ASA) devices and forwards them to Cisco SAL in the cloud. Installation instructions can be found here. While SEC remains the most scalable route to send logs to SAL (SaaS), firewall devices running Cisco Firepower version 6.5 or later can send event logs directly to SAL Cloud, without the need for an SEC. This capability has been found to reliably support sustained peak rates of up to 8,500 events per second (eps) per firewall device. The Cisco Firewall Management Center (FMC) version 7.0 supports this direct- to-cloud route of devices under its management through its “Integrations” settings.

Platform support matrix: Cisco security devices supported by Security Cloud Control

Cisco security devices supported by Security Cloud Control

Product	ASA software version	FTD version
ASAv	8.4 and later	N/A
ASA 5506-X, ASA 5512-X	8.4 and later	N/A
ASA 5525-X, 5545-X, 5555-X	8.4 and later	N/A
ASA 5585-10, 5585-20, 5585-40, 5585-60	8.4 and later	N/A
ISA 3000	8.4 and later	7.0.3 and later (excluding 7.1)
Firepower 1010, Firepower 1120, Firepower 1140, Firepower 1150	9.8 and later	7.0.3 and later (excluding 7.1)
Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140	9.8 and later	7.0.3 and later (excluding 7.1)
Firepower 3105, Firepower 3110, Firepower 3120, Firepower 3130, Firepower 3140	9.17.1 for 3100, 3120, 3130 and 3140, 9.19.1 for 3105 and later	7.1 and later
Firepower 4112, Firepower 4115, Firepower 4125, Firepower 4145,	9.4 and later	7.0.3 and later (excluding 7.1)
Firepower 4215, Firepower 4225, Firepower 4245	9.20 and later	7.4 and later
Firepower 9300	9.4 and later	7.0.3 and later (excluding 7.1)
FTDv: KVM, VMware, Azure	NA	7.0.3 and later (excluding 7.1)
Meraki MX	NA	NA
Cisco IOS (SSH): Limited to CLI Tool and Change Log Only	NA	NA

Ordering information

Firewall management/Multi cloud defense for Security Cloud Control (SCC) requires a base subscription for tenant entitlement that covers ASA, FTD and Multicloud Defense. For Firewall customers, there will be per-device license subscription for device management entitlement. The Device License Subscription with unlimited logging subscription is available separately. Subscriptions of one, three, and five years are available.

For Multicloud Defense, the product licensing is based on the consumed amount of aggregated gateway hours across all the cloud environments. The product has two tiers available, namely, Advantage and Premier. Firewall device licenses, such as Threat, Malware, URL filtering, and support, should be purchased separately. Security Logging and Analytics can also be added for logging and troubleshooting use cases.

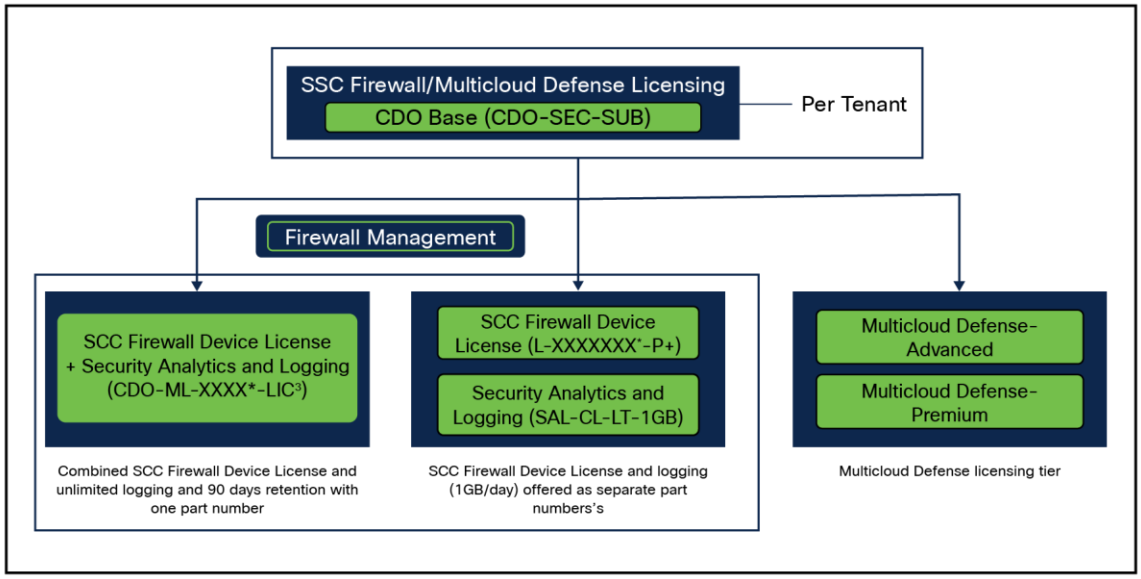

Figure 8.
Firewall management/Multi cloud defense for Security Cloud Control licensing structure

*denotes the firepower model. For example, if you are ordering 10 Cisco FPR1010 devices and want to manage these devices from SCC Firewall device license with unlimited logging and 90 days retention, the part number will be CDO-ML-FP1010-LIC along with CDO-SEC-SUB (tenant entitlement). Another example, if you are ordering 10 Cisco FPR3110 devices and want to manage these devices from SCC with separate logging (1GB/day), there will be 2 part numbers - L-FPR3110-P= and SAL-CL-LT-1GB along with CDO-SEC-SUB (tenant entitlement). Relevant subscription term to be chosen.

Refer to Guidelines for Quoting Security Cloud control Products Ordering Guide for more information on ordering Security Cloud Control. To place an order, visit the Cisco ordering homepage.

Table 2. Firewall Management/Multicloud defense for Security Cloud Control Xaas license for tenant entitlement

Part number	Description
CDO-SEC-SUB	SCC Firewall/Multicloud defense XaaS Subscription

Table 3. Firewall Management/Multicloud defense for Security Cloud Control Base License Subscription tenant entitlement: subscription of 1, 3, and 5 years available

Part number	Description
CDO-BASE-LIC	SCC Firewall/Multi cloud defense Base License Subscription

Table 4. SAL Saas logging and troubleshooting XaaS license for logging entitlement

Part number	Description
SAL-SUB	SAL Xaas Subscription

Table 5. Firewall Management for Security Cloud Control license for managing Cisco firewalls: subscription of 1, 3, and 5 years available

Part number	Description
L-FPR1010-P=	SCC Firewall Device license for FPR1010 running ASA or FTD Image
L-FPR1120-P=	SCC Firewall Device license for FPR1120 running ASA or FTD Image
L-FPR1140-P=	SCC Firewall Device license for FPR1140 running ASA or FTD Image
L-FPR1150-P=	SCC Firewall Device license for FPR1150 running ASA or FTD Image
L-ASA5505-P=	SCC Firewall Device license for ASA 5505 running ASA or FTD Image
L-ASA5506-P=	SCC Firewall Device license for ASA 5506 running ASA or FTD Image
L-ASA5506W-P=	SCC Firewall Device license for ASA 5506W running ASA or FTD Image
L-ASA5506H-P=	SCC Firewall Device license for ASA 5506H running ASA or FTD Image
L-ASA5508-P=	SCC Firewall Device license for ASA 5508 running ASA or FTD Image
L-ASA5512-P=	SCC Firewall Device license for ASA 5512 running ASA or FTD Image
L-ASA5525-P=	SCC Firewall Device license for ASA 5525 running ASA or FTD Image
L-ASA5545-P=	SCC Firewall Device license for ASA 5545 running ASA or FTD Image
L-ASA5555-P=	SCC Firewall Device license for ASA 5555 running ASA or FTD Image
L-ASA5585-P=	SCC Firewall Device license for ASA 5585 running ASA or FTD Image
L-ASAV-P=	SCC Firewall Device license for Cisco Adaptive Security Virtual Appliance (ASAv)
L-FPRTD-V-P=	SCC Firewall Device license for Virtual FTD (FTDv5/10/20/30/50/100)

Part number	Description
L-FPR2110-P=	SCC Firewall Device license for FPR 2110 running ASA or FTD Image
L-FPR2120-P=	SCC Firewall Device license for FPR 2120 running ASA or FTD Image
L-FPR2130-P=	SCC Firewall Device license for FPR 2130 running ASA or FTD Image
L-FPR2140-P=	SCC Firewall Device license for FPR 2140 running ASA or FTD Image
L-FPR3105-P=	SCC Firewall Device license for FPR 3105 running ASA or FTD Image
L-FPR3110-P=	SCC Firewall Device license for FPR 3110 running ASA or FTD Image
L-FPR3120-P=	SCC Firewall Device license for FPR 3120 running ASA or FTD Image
L-FPR3130-P=	SCC Firewall Device license for FPR 3130 running ASA or FTD Image
L-FPR3140-P=	SCC Firewall Device license for FPR 3140 running ASA or FTD Image
L-FPR4112-P=	SCC Firewall Device license for FPR 4112 running ASA or FTD Image
L-FPR4115-P=	SCC Firewall Device license for FPR 4115 running ASA or FTD Image
L-FPR4125-P=	SCC Firewall Device license for FPR 4125 running ASA or FTD Image
L-FPR4145-P=	SCC Firewall Device license for FPR 4145 running ASA or FTD Image
L-FPR4215-P=	SCC Firewall Device license for FPR 4215 running ASA or FTD Image
L-FPR4225-P=	SCC Firewall Device license for FPR 4225 running ASA or FTD Image
L-FPR4245-P=	SCC Firewall Device license for FPR 4245 running ASA or FTD Image
L-FPR-9K-P=	SCC Firewall Device license for FPR 9300 Series running ASA or FTD Image
L-ISA3000-P=	SCC Firewall Device license for ISA 3000 running ASA or FTD Image
L-MX64-P=	SCC Firewall Device license for Meraki MX64 Platform
L-MX65-P=	SCC Firewall Device license for Meraki MX65 Platform
L-MX67-P=	SCC Firewall Device license for Meraki MX67 Platform
L-MX84-P=	SCC Firewall Device license for Meraki MX84 Platform
L-MX100-P=	SCC Firewall Device license for Meraki MX100 Platform
L-MX250-P=	SCC Firewall Device license for Meraki MX250 Platform
L-MX450-P=	SCC Firewall Device license for Meraki MX450 Platform
L-AWS-SG=	SCC Firewall Device license for Amazon Web Services VPC Security Group

Table 6. SCC Firewall Device license for managing Cisco firewalls with unlimited logging and 90 days retention: subscription of 1, 3, and 5 years available.

Part number	Description
CDO-ML-FP1010-LIC	SCC Firewall Device license with logging FPR 1010 ASA or FTD Image
CDO-ML-FP1010E-LIC	SCC Firewall Device license with logging FPR 1010E ASA or FTD Image
CDO-ML-FP1120-LIC	SCC Firewall Device license with logging for FPR 1120 ASA or FTD Image
CDO-ML-FP1140-LIC	SCC Firewall Device license with logging for FPR 1140 ASA or FTD Image
CDO-ML-FP1150-LIC	SCC Firewall Device license with logging for FPR 1150 ASA or FTD Image
CDO-ML-FP2110-LIC	SCC Firewall Device license with logging for FPR 2110 ASA or FTD Image
CDO-ML-FP2120-LIC	SCC Firewall Device license with logging for FPR 2120 ASA or FTD Image
CDO-ML-FP2130-LIC	SCC Firewall Device license with logging for FPR 2130 ASA or FTD Image
CDO-ML-FP2140-LIC	SCC Firewall Device license with logging for FPR 2140 ASA or FTD Image
CDO-ML-FP3105-LIC	SCC Firewall Device license with logging for FPR 3105 ASA or FTD Image
CDO-ML-FP3110-LIC	SCC Firewall Device license with logging for FPR 3110 ASA or FTD Image
CDO-ML-FP3120-LIC	SCC Firewall Device license with logging for FPR 3120 ASA or FTD Image
CDO-ML-FP3130-LIC	SCC Firewall Device license with logging for FPR 3130 ASA or FTD Image
CDO-ML-FP3140-LIC	SCC Firewall Device license with logging for FPR 3140 ASA or FTD Image
CDO-ML-FP4112-LIC	SCC Firewall Device license with logging for FPR 4112 ASA or FTD Image
CDO-ML-FP4115-LIC	SCC Firewall Device license with logging for FPR 4115 ASA or FTD Image
CDO-ML-FP4125-LIC	SCC Firewall Device license with logging for FPR 4125 ASA or FTD Image
CDO-ML-FP4145-LIC	SCC Firewall Device license with logging for FPR 4145 ASA or FTD Image
CDO-ML-FP4215-LIC	SCC Firewall Device license with logging for FPR 4215 ASA or FTD Image
CDO-ML-FP4225-LIC	SCC Firewall Device license with logging for FPR 4225 ASA or FTD Image
CDO-ML-FP4245-LIC	SCC Firewall Device license with logging for FPR 4245 ASA or FTD Image
CDO-ML-F9K-S40-LIC	SCC Firewall Device license with logging for FPR 9K-SM40 ASA or FTD Image
CDO-ML-F9K-S48-LIC	SCC Firewall Device license with logging for FPR 9K-SM48 ASA or FTD Image
CDO-ML-F9K-S56-LIC	SCC Firewall Device license with logging for FPR 9K-SM56 ASA or FTD Image
CDO-ML-FTDV5-LIC	SCC Firewall Device license with logging for FTDV Base Lic,100Mbps
CDO-ML-FTDV10-LIC	SCC Firewall Device license with logging for FTDV Base Lic, 1Gbps

Part number	Description
CDO-ML-FTDV20-LIC	SCC Firewall Device license with logging for FTDV Base Lic, 3Gbps
CDO-ML-FTDV30-LIC	SCC Firewall Device license with logging for FTDV Base Lic, 5Gbps
CDO-ML-FTDV50-LIC	SCC Firewall Device license with logging for FTDV Base Lic, 10Gbps
CDO-ML-FTDV100-LIC	SCC Firewall Device license with logging for FTDV Base Lic, 16Gbps

Table 7. Cisco Logging and Troubleshooting with subscription of 1, 3, and 5 years available

Part number	Description
SAL-CL-LT-1GB	License Logging and Troubleshooting for 1GB/day
SAL-CL-LT-OVRG	Usage-based overage PID for License Logging and Troubleshooting, not charged at time of placing order but is used to calculate overage charges if entitlement is exceeded.
SEC-LOG-CL	Cloud logging with 90 days storage -GB/day
SAL-CL-1GB-(1/2/3)Y-EXTN*	1/2/3 year of logs retention (up from default of 90 days).
SEC-CL-DR-(1/2/3)Y*	Data Retention extensions, which extend log retention to 1, 2, or 3 years in the cloud.
SAL-CL-LT-1GB	License Logging and Troubleshooting for 1GB/day

*Log retention period can optionally be extended to 1, 2, or 3 years

Security Buying Programs

The offer leverages the Security Choice Enterprise Agreement buying program with the following PIDs: The mapping for Choice EA PIDs to CDO, SAL (SaaS) a-la-carte PIDs.

Table 8.

EA 2.0 ATO	EA 2.0 Billing PID	EA 3.0 ATO	EA 3.0 Billing PID	A-la-carte Fulfillment PID
E2F-SEC-CDO	E2SF-O-CDO55s08P	E3-SEC-CDO	E3S-CDO5508P	L-ASA5508-P=
E2F-SEC-CDO	E2SF-O-CDO5516P	E3-SEC-CDO	E3S-CDO5516P	L-ASA5516-P=
E2F-SEC-CDO	E2SF-O-CDO5525P	E3-SEC-CDO	E3S-CDO5525P	L-ASA5525-P=
E2F-SEC-CDO	E2SF-O-CDO5545P	E3-SEC-CDO	E3S-CDO5545P	L-ASA5545-P=
E2F-SEC-CDO	E2SF-O-CDO5555P	E3-SEC-CDO	E3S-CDO5555P	L-ASA5555-P=
E2F-SEC-CDO	E2SF-O-CDO-BASE	E3-SEC-CDO	E3S-O-CDO-BASE	CDO-BASE-LIC
E2F-SEC-CDO	E2SF-O-CDOFPR9K	E3-SEC-CDO	E3S-CDOFPR9K	L-FPR-9K-P=
E2F-SEC-CDO	E2SF-O-FPR1010-P	E3-SEC-CDO	E3S-CDOFPR1010-P	L-FPR1010-P=
E2F-SEC-CDO	E2SF-O-FPR1120-P	E3-SEC-CDO	E3S-CDOFPR1120-P	L-FPR1120-P=

EA 2.0 ATO	EA 2.0 Billing PID	EA 3.0 ATO	EA 3.0 Billing PID	A-la-carte Fulfillment PID
E2F-SEC-CDO	E2SF-O-FPR1140-P	E3-SEC-CDO	E3S-CDOFPR1140-P	L-FPR1140-P=
E2F-SEC-CDO	E2SF-O-FPR1150-P	E3-SEC-CDO	E3S-CDOFPR1150-P	L-FPR1150-P=
E2F-SEC-CDO	E2SF-O-FPR2110-P	E3-SEC-CDO	E3S-CDOFPR2110-P	L-FPR2110-P=
E2F-SEC-CDO	E2SF-O-FPR2120-P	E3-SEC-CDO	E3S-CDOFPR2120-P	L-FPR2120-P=
E2F-SEC-CDO	E2SF-O-FPR2130-P	E3-SEC-CDO	E3S-CDOFPR2130-P	L-FPR2130-P=
E2F-SEC-CDO	E2SF-O-FPR2140-P	E3-SEC-CDO	E3S-CDOFPR2140-P	L-FPR2140-P=
E2F-SEC-CDO	E2SF-O-FPR3110-P	E3-SEC-CDO	E3S-CDOFPR3110-P	L-FPR3110-P=
E2F-SEC-CDO	E2SF-O-FPR3120-P	E3-SEC-CDO	E3S-CDOFPR3120-P	L-FPR3120-P=
E2F-SEC-CDO	E2SF-O-FPR3130-P	E3-SEC-CDO	E3S-CDOFPR3130-P	L-FPR3130-P=
E2F-SEC-CDO	E2SF-O-FPR3140-P	E3-SEC-CDO	E3S-CDOFPR3140-P	L-FPR3140-P=
E2F-SEC-CDO	E2SF-O-FPR4110-P	E3-SEC-CDO	E3S-CDOFPR4110-P	L-FPR4110-P=
E2F-SEC-CDO	E2SF-O-FPR4112-P	E3-SEC-CDO	E3S-CDOFPR4112-P	L-FPR4112-P=
E2F-SEC-CDO	E2SF-O-FPR4115-P	E3-SEC-CDO	E3S-CDOFPR4115-P	L-FPR4115-P=
E2F-SEC-CDO	E2SF-O-FPR4120-P	E3-SEC-CDO	E3S-CDOFPR4120-P	L-FPR4120-P=
E2F-SEC-CDO	E2SF-O-FPR4125-P	E3-SEC-CDO	E3S-CDOFPR4125-P	L-FPR4125-P=
E2F-SEC-CDO	E2SF-O-FPR4140-P	E3-SEC-CDO	E3S-CDOFPR4140-P	L-FPR4140-P=
E2F-SEC-CDO	E2SF-O-FPR4145-P	E3-SEC-CDO	E3S-CDOFPR4145-P	L-FPR4145-P=
E2F-SEC-CDO	E2SF-O-FPR4150-P	E3-SEC-CDO	E3S-CDOFPR4150-P	L-FPR4150-P=
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-1Y	E3-SEC-SAL-LT	E3S-SALLT-STG-1Y	SAL-CL-1GB-1Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-2Y	E3-SEC-SAL-LT	E3S-SALLT-STG-2Y	SAL-CL-1GB-2Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-3Y	E3-SEC-SAL-LT	E3S-SALLT-STG-3Y	SAL-CL-1GB-3Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SAL-ESS	E3-SEC-SAL-LT	E3S-SAL-LT	SAL-CL-LT-1GB

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

Cisco Defense Orchestrator, learn more.

Firewall Management Center, learn more.

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 C78-736847-16 11/24