ANM TECH DAY

Hybrid Mesh Firewalls

Where Enforcement Lives in a Distributed World

ANM Tech Day

Kevin Snoddy

Cybersecurity Solutions Architect

- 30+ years of experience designing and implementing secure, scalable solutions
- Extensive background in network security, SSE/SASE, route/switch, SD-WAN, and wireless
- 15+ years partnering with customers to solve complex business and security challenges, with deep expertise in security architecture, Zero Trust, and network transformation
- 15+ years in the K-12 sector as a customer, with first-hand insight into the operational and security challenges facing educational institutions
- Passionate about aligning security strategies with business objectives
- Focused on collaborative, customer-centric solutions that support organizational goals
- Committed to educating and empowering teams for long-term security success
- Outside of work, I enjoy all forms of motorsports, spending time outdoors, and hunting

www.linkedin.com/i/in/kevinsnoddy/

What We Will Discuss Today

1

How We Got Here

How the network evolved — and why the security model didn't keep up.

2

Hybrid Mesh Firewall

Gartner's definition, what it requires, and why it matters now and HMF ROI

3

Palo Alto's Architecture

How Palo Alto approaches hybrid mesh
Forrester TEI Study

.

4

Cisco's Architecture

How Cisco approaches hybrid mesh
Forrester TEI Study
.

5

Key Takeaways

What you should walk out knowing and what to do with it.
.

6

How ANM can help

Workshops
Tools Rationalization

The Network Changed. The Security Model Didn't.

Pre-2007

On-Prem Only

Perimeter firewall. One edge. Security model matches the network.

2007-2010

Virtualization

East-west traffic explodes inside the DC. Perimeter firewall sees none of it.

2011-Present

Cloud Adoption

Workloads move to AWS, Azure, GCP. VPNs and cloud-native controls create policy silos.

2025-Present

Hybrid Mesh

Every user, every app, every location. Threats move between enforcement gaps.

WHY THE OLD SECURITY MODEL BROKE

Threat Sophistication

Attackers don't hit the perimeter anymore. They get in through phishing, compromised credentials, or supply chain — then move laterally across domains your perimeter firewall never inspects.

Encrypted Traffic

Over 95% of web traffic is now TLS encrypted. Your firewall can't inspect what it can't see. SSL inspection at scale requires compute your original architecture wasn't sized for.

Attack Surface Expansion

Every cloud workload, remote user, and IoT device is an entry point. The attack surface grew 10x. The security model didn't keep up.

Hybrid Mesh Firewall:

Gartner Definition

A hybrid mesh firewall is a firewall platform that provides policy management and enforcement across multiple form factors — physical appliances, virtual machines, cloud-native, and SaaS-delivered — from a unified management plane. It enables consistent security policy across on-premises, branch, cloud, and remote access environments, supporting zero trust network access principles across the full enterprise traffic flow.

Source: Gartner, Market Guide for Hybrid Mesh Firewalls

What That Actually Requires

Distributed Enforcement

Policy at every edge, cloud gateway, and internal segment — not just the perimeter.

SSL/TLS at Scale

95%+ of traffic is encrypted. You need to inspect it without killing throughput.

Unified Management

Single pane across all form factors. Human-scale control requires unified visibility.

Consistent Policy Engine

One framework across physical, virtual, and cloud-native. No drift between domains.

App & User Context

App-ID and User-ID across every enforcement point. Context drives policy, not IP and port.

Automated Response

Threats move faster than humans. Enforcement needs to respond to telemetry in near real-time.

What Changes for Your Environment

01

You're routing and switching decisions now directly affect security enforcement boundaries.

02

Unified management isn't a nice-to-have — it's the operational difference between a repeatable process and a daily firefight.

03

SD-WAN and SASE aren't separate conversations anymore — policy enforcement rides the same path as traffic.

04

If your firewall only sits at the edge, it misses everything happening inside. East-west needs enforcement at the hypervisor or fabric layer

05

SSL/TLS decryption must be designed into the architecture — not bolted on after the fact. Right-sizing appliances to absorb the inspection overhead works on-prem, but cloud-delivered enforcement gives you decryption at cloud scale without the hardware conversation.

Hybrid Mesh Firewalls ROI

GARTNER

Market Adoption

60%+

of organizations will have **multiple firewall deployments**

by 2026

Enterprises managing multiple firewall deployments are driving rapid adoption of Hybrid Mesh Firewall architectures.

Source: Gartner Market Guide for Hybrid Mesh Firewall

IDC 2026

ROI & Cost Savings

314%
3-year ROI

6-Month Payback Period
on initial investment

25% Cost Reduction
from consolidating point products into one platform

$14.18M in benefits vs. $3.43M invested

Source: IDC Business Value Study, 2026 (commissioned by Check Point)

IDC 2026

Security Outcomes

78% **faster**
Time to Incident Resolution

66% **reduction in**
Business Downtime Annually

54% **less staff time**
Required for Security Patching

Fewer incidents. Faster recovery.
More time for what matters.

Source: IDC Business Value Study, 2026 (commissioned by Check Point)

HMF Misconceptions

- **HMFs are too complex for most organizations.**
  - Most of the complexity in network security comes from managing multiple firewall products separately.
- **You only need a Hybrid mesh firewalls if you have a large, global network.**
  - HMFs are designed for hybrid environments. Not just large ones.
- **Centralized control means giving up flexibility.**
  - Centralized control means having one place to define policies. And the flexibility to apply them based on context.
- **It's easier to stick with traditional firewalls & layer on extra tools**
  - Point solutions create overlap, blind spots, and policy drift.

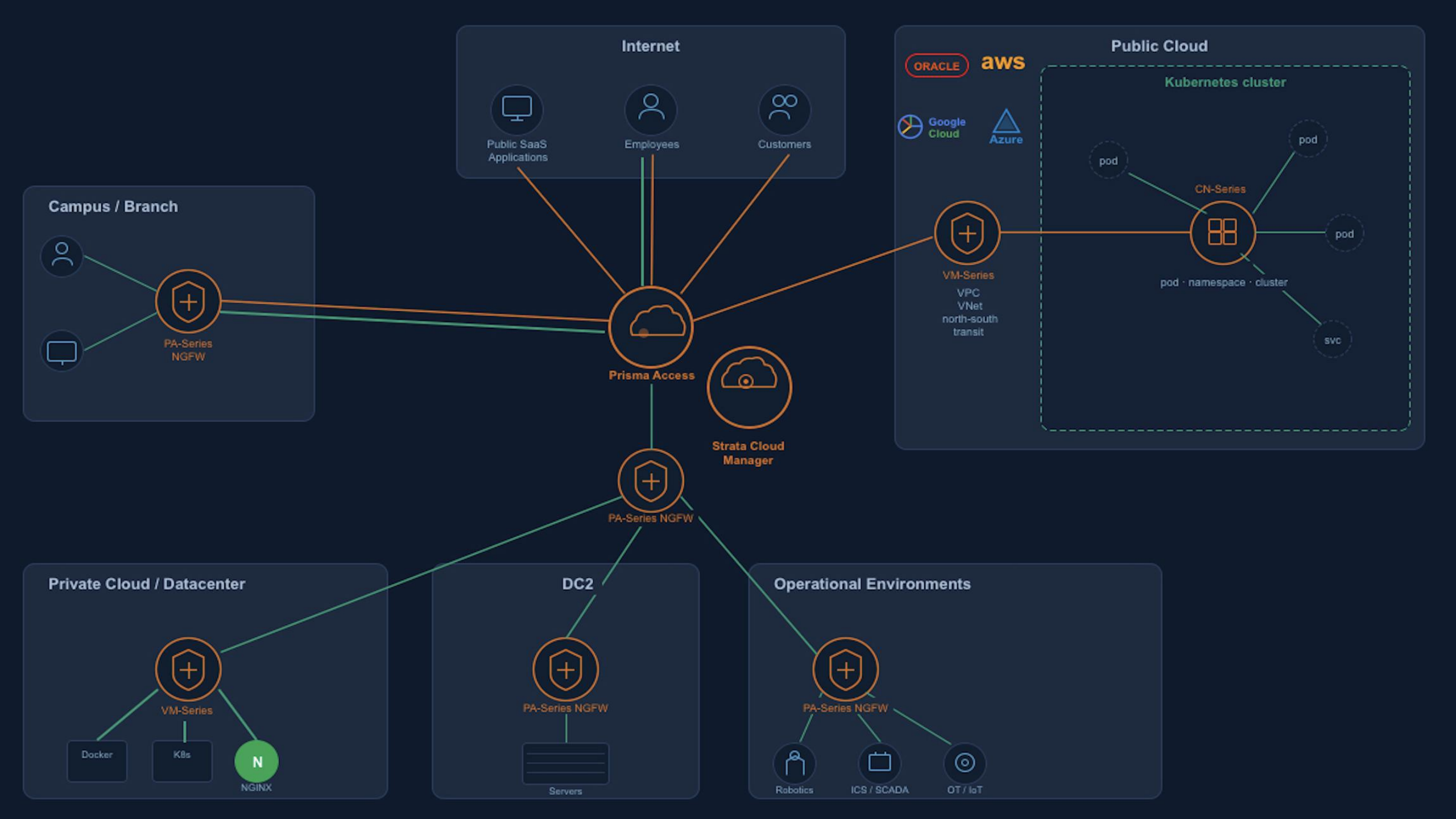
Palo Alto’s Architecture

How Palo Alto builds a hybrid mesh firewall and where it fits

Palo Alto's Hybrid Mesh Firewall Architecture

Palo Alto Hybrid Mesh Firewall Core Components:

Management Layer **Strata Cloud Manager (SCM)**	AI-driven, cloud-delivered management for all PA-Series NGFWs. Provides Best Practice Assessment, autonomous policy optimization, and unified visibility across all form factors without on-prem management infrastructure.
Enforcement Layer **PA-Series NGFWs + VM-Series + CN-Series**	Physical (PA-400 through PA-7500), virtual (VM-Series), and container-native (CN-Series) form factors. Same PAN-OS across all — true consistent enforcement.
Detection & Response **Cortex XDR + XSIAM**	Purpose-built XDR with native integration into firewall telemetry. XSIAM consolidates SIEM, SOAR, and threat intel into one AI-driven platform.
Access & Identity **Prisma Access + Prisma Access Browser + CyberArk**	Cloud-delivered ZTNA, CASB, and SWG for remote access and branch. Natively integrated with PA-Series policy. CyberArk sits separate from the core firewall stack — additional licensing required.


Internet
Public SaaS Applications
Employees
Customers
Public Cloud
ORACLE
aws
Google Cloud
Azure
Kubernetes cluster
pod
pod
CN-Series
pod
pod · namespace · cluster
svc
VM-Series
VPC
VNet
north-south
transit
Campus / Branch
PA-Series NGFW
Prisma Access
Strata Cloud Manager
PA-Series NGFW
Private Cloud / Datacenter
VM-Series
Docker
K8s
N
NGINX
DC2
PA-Series NGFW
Servers
Operational Environments
PA-Series NGFW
Robotics
ICS / SCADA
OT / IoT

CUSTOMER CASE STUDY

Palo Alto Networks Strata — Hybrid Mesh Firewall in Practice

Palo Alto Networks | Strata Platform

Forrester TEI Study, 2024

THE CHALLENGE

Enterprise organizations managing multiple firewall vendors across on-premises data centers, branch offices, and multi-cloud environments faced fragmented visibility, inconsistent policy enforcement, and high operational overhead.

- Siloed management consoles across hardware, VM, and cloud FWs
- Manual policy synchronization driving compliance risk
- Threat visibility gaps between environments

THE SOLUTION

Deployed the Strata Security Platform — a unified Hybrid Mesh Firewall consolidating hardware NGFWs, VM-Series, CN-Series, and Prisma Access under a single Strata Cloud Manager pane of glass with AI-powered threat prevention.

RESULTS

174%

Return on Investment

Over 3 years (Forrester TEI, 2024)

$26.2M

Net Present Value

3-year benefit to composite org

<6 mo

Payback Period

Time to recoup full investment

$331K

Annual savings in security ops costs

90%

Reduction in data center power & HVAC costs

"Consolidating our firewall estate onto Strata eliminated tool sprawl and gave us consistent enforcement from campus to cloud."

Source: Forrester Consulting Total Economic Impact™ Study, commissioned by Palo Alto Networks, Oct 2024

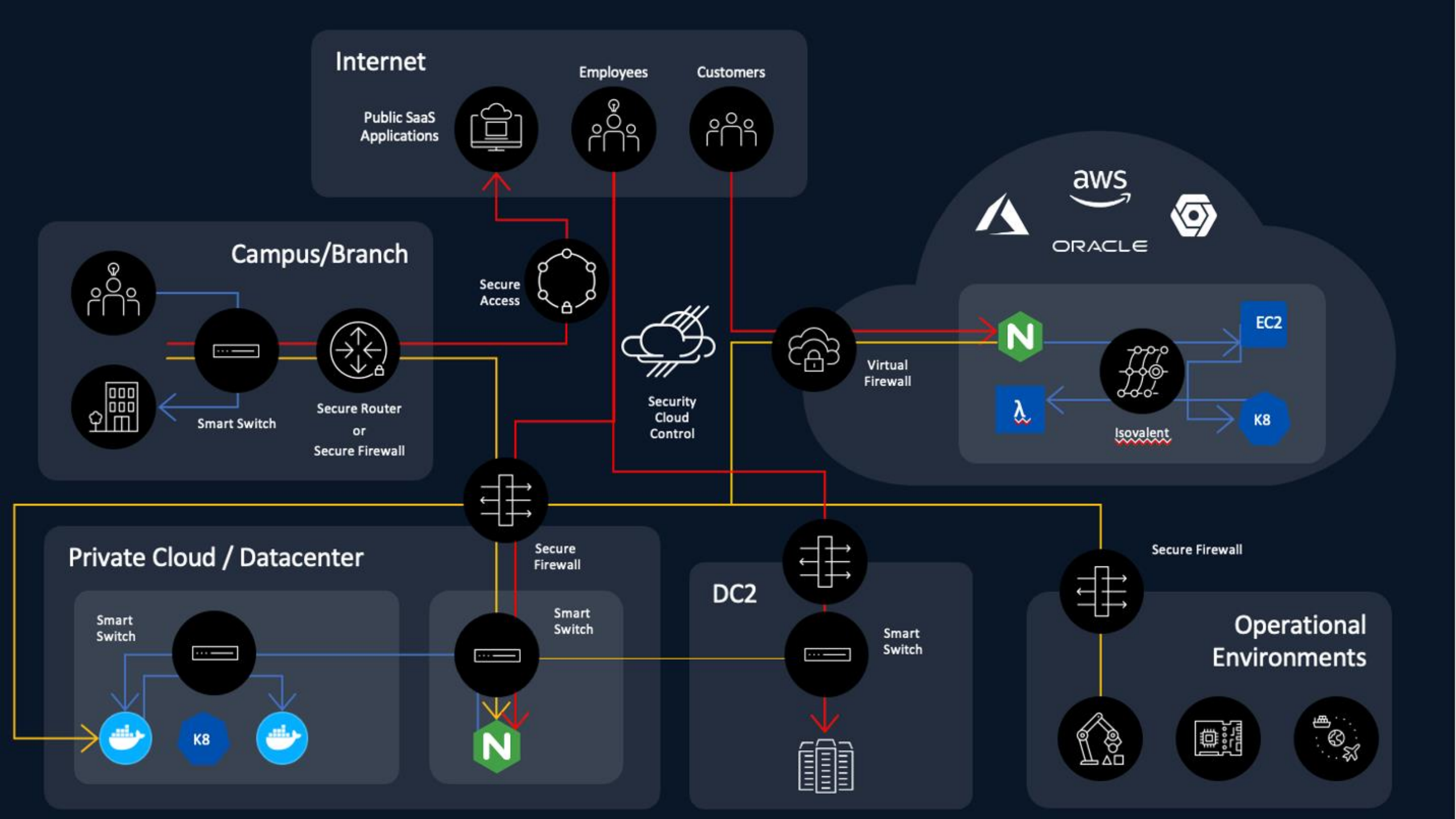
Cisco’s Architecture

How Cisco builds a hybrid mesh firewall and where it fits

Cisco's Hybrid Mesh Firewall

Cisco Hybrid Mesh Firewall Core Components:

Management Layer Security Cloud Control	Unified policy management across all Cisco NGFW form factors — physical, virtual, and cloud-native.
Enforcement Layer Cisco Secure Firewall — FTD, FTDv, N9K Smart Switch, Multi-Cloud Defense and Secure Workload	Distributed enforcement across data center, multi-cloud (AWS, Azure, GCP), and branch. Consistent Snort 3 inspection engine across all form factors.
Detection & Response Cisco XDR + Secure Endpoint	Telemetry aggregation across network and endpoint. Closed-loop response feeds back into firewall enforcement.
Access & Identity Cisco Secure Access (SSE) + Duo + Cisco ISE	Zero Trust access layer for remote users and cloud apps. ISE provides network access control and segmentation policy enforcement on-prem. Duo sits separate from the core firewall stack — additional licensing required.


Internet
Public SaaS Applications
Employees
Customers
Campus/Branch
Secure Access
Smart Switch
Secure Router or Secure Firewall
Security Cloud Control
Virtual Firewall
aws
ORACLE
EC2
K8
Isovalent
Private Cloud / Datacenter
Smart Switch
K8
Secure Firewall
Smart Switch
DC2
Smart Switch
Secure Firewall
Operational Environments

CUSTOMER CASE STUDY

Cisco Secure Firewall — Hybrid Mesh Firewall in Practice

Cisco | Secure Firewall + CDO

Forrester TEI Study, 2022

THE CHALLENGE

Enterprise organizations managing multiple firewall vendors across on-premises data centers, branch offices, and multi-cloud environments faced fragmented visibility, inconsistent policy enforcement, and high operational overhead.

- Siloed management consoles across hardware, VM, and cloud FWs
- Manual policy synchronization driving compliance risk
- Threat visibility gaps between environments

THE SOLUTION

Deployed Cisco Secure Firewall — a unified Hybrid Mesh Firewall consolidating hardware appliances, FTDv, and cloud-native FTD under a single Security Cloud Control pane of glass with integrated IPS, malware defense, and XDR.

RESULTS

195%

Return on Investment

Over 3 years (Forrester TEI, 2022)

$12.3M

Net Present Value

3-year benefit to composite org

<12 mo

Payback Period

Time to recoup full investment

95%
Reduction in network/security ops work streams

83%
Faster threat response time

"Managing our firewall fleet through a single console eliminated the policy gaps that were keeping us up at night."

Source: Forrester Consulting Total Economic Impact™ Study, commissioned by Cisco, Mar 2022

What You Should Walk Away Thinking About

01

Your perimeter firewall doesn't see most of your traffic anymore

East-west, cloud-to-cloud, and SaaS-bound traffic can bypass it entirely. Enforcement must follow the traffic, not wait for it at the edge.

02

Policy consistency across products is harder than it sounds

Different enforcement points with different policy engines means drift. Drift means gaps. Gaps are where lateral movement lives.

03

Disconnected enforcement points compound complexity — they don't scale.

Every enforcement point you add without unified management becomes its own maintenance problem.

04

SSL/TLS decryption is an architecture decision, not just a sizing decision

You can right-size appliances to absorb the inspection overhead, or offload decryption to a cloud-delivered enforcement point that scales on demand. Either way, it has to be designed in — not bolted on after the fact.

05

The architecture decision you make today shapes your options for years

Whether you integrate into existing infrastructure or consolidate onto a new platform, the choice affects how you add enforcement points, manage policy, and respond to incidents going forward.

How Can ANM Help?

- **Tools Rationalization:** Inventory your technology stack, map the overlaps, and build a roadmap that reduces cost and complexity.
- **Workshops:** Map your environment with key stakeholders. Identify the gaps before they become incidents.

Ready to start?

Contact your ANM Account Manager and schedule a workshop for your organization

Kevin Snoddy
Cybersecurity Solutions Architect
Kein.snoddy@anm.com
www.linkedin.com/i/in/kevinsnoddy/