Playbook
Cisco Partner Confidential

Cisco Network Firewalls

Sales Playbook

Table of contents

Introduction

Cisco Next-Generation Firewalls (NGFWs)

Purpose

This playbook is meant to make it easy for you to introduce and sell Cisco's Next-Generation Firewalls (NGFWs) and associated network security portfolio. It will equip Cisco Partners with the knowledge to effectively engage customers about the benefits of an integrated security platform with Cisco NGFW as the cornerstone, and the positioning and messaging to ensure it aligns with Cisco's in-market campaigns.

Objectives

- Provide guidance for engaging customers in discussions about Cisco NGFW solutions
- Share market insights driving demand for integrated security solutions
- Discuss why next generation firewalls are important to your customers
- Review customer scenarios and business drivers for Cisco NGFW
- Identify integrated security opportunities within your accounts for purchasing a Cisco NGFW

Key Takeaways

Customers are evaluating their security posture to safeguard against the expanding threat landscape. It's an ideal opportunity to discuss refreshing their security with Cisco firewalls at the center. This playbook will help you:

- Build your pipeline
- Protect your customers' business with threat-focused security
- Displace and exclude competition
- Establish yourself as a trusted advisor for future business opportunities

Introduction (cont.)

Context

Today, there no longer is a single network perimeter or control point. Instead, we have multiple "micro-perimeters" across a variety of interconnected networks, devices, users, and data. Consequently, our "traditional" firewall devices are being augmented by a mixture of physical and virtual appliances across an increasingly interconnected and complex environment. As a result, organizations are struggling to operationalize disparate security solutions to maintain consistent policies and uniform threat visibility.

It's time to re-think the firewall

Your customers need an integrated security approach to deliver world-class security controls everywhere, with consistent visibility, policy harmonization, and stronger user and device authentication.

Our NGFW messaging is anchored around these three pillars:

- Turn your entire network into an extension of security architecture
- World-class security controls
- Unified policy and threat visibility

Elevator Pitch

Your customers face a constantly changing threat landscape and the evolving network is part of the problem. Cisco NGFW is the foundation that turns their network into the solution.

The Cisco NGFW portfolio delivers world-class security controls backed by industry-leading threat intelligence, with consistent security policies
and visibility.

Let your customer's take control of their security landscape, from the data center, branch offices, cloud environments, and everywhere in between. They can leverage existing investments in Cisco to start turning their network infrastructure into additional control points and a
direct extension of their firewall solution, leading to a complete
security architecture.

Opportunity

Why This Matters to Customers

Existing security solution is too complex, ineffective and not future-ready.

- Organizations are using disparate and disconnected point security products
- This is leading to unnecessary complexity
- IT staff is constrained with limited visibility
- The usage of cloud services and IoT devices are exploding, leading to more de-centralized IT assets that are inherently more difficult to secure

Why This Matters to You

Safeguarding a business’ most value assets will ensure you are their service provider of choice today and tomorrow.

- That includes network, data, endpoints and protecting the brand is a priority at the executive level
- As you educate your customers on future-proofing their enterprise, you can expand your footprint with existing Cisco security customers and grow your customer base

Market Opportunity

Industry Trends

Existing Cisco customers

- Cisco ASA install base is a $1.6B opportunity that is approaching a refresh cycle
- Per Gartner, firewalls are on a five-year refresh cycle

Customers using a competitor's firewall

- NGFW Market Soaring at 12.9% CAGR to $6.7M by 2025
- Per PR Newswire, the global network firewall market is expected to reach $6 billion by 2024
- Every customer that switches to Cisco NGFW opens the door for new revenue opportunity for Cisco networking products, and more

De-centralization of IT assets

IT assets are moving out of the data center and into the cloud.

- 70% Enterprise organizations are currently migrating enterprise resource planning (ERP) applications to the cloud.
- By 2021, more than half of global enterprises already using cloud today will adopt an all-in cloud strategy.
- Nearly 83 percent of enterprises will rely on the cloud by the end of this decade.

Network security management complexity

Organizations have accumulated a variety of different network security products to protect against a growing attack surface creating a burden for the IT team.

- The average enterprise has 75 security tools.
- 82% of companies want an integrated security portfolio.
- Shadow IT is 30 to 40 percent of IT spending in large enterprises.

Rise in encrypted traffic

Encryption is the primary method of securing information, but it consumes firewall processing resources.

- 94% of all Google web traffic? is encrypted.
- Nearly 80% of web pages loaded by Firefox use HTTPS.

Reasons to Upgrade

Better performance

- 3.5x performance boost in NGFW throughput
- Up to 5x boost in VPN throughput

More connections

- Up to 2x more connections per second (CPS)

Improved encrypted traffic throughput

- Up to 3x performance boost in encrypted traffic performance compared to legacy models

Future-proof your network

- Consistent visibility, policy harmonization, and cloud management
- Improved threat protection

Existing Cisco firewall customers

By upgrading to a new Cisco firewall appliance today, your customers will gain higher capacity and better performance.

The Cisco NGFW is the foundation to future-proof their network with consistent visibility, policy harmonization, and cloud management.

Your customers can improve threat response and protection from even the most sophisticated threats with a Cisco NGFW for the strongest security posture today and tomorrow.

Flexible upgrade options.

- ASA base code is supported on Cisco NGFW to provide familiar tools
- Upgrade to a Firepower Threat Defense (FTD) platform later to take advantage of advanced threat protection

These are the Cisco ASA 5500-X Series models that are being refreshed: 5506, 5508, 5516, 5525, 5545, 5555

Reasons to Switch to Cisco

Modern security architecture

- Fully integrated platform
- Product breadth and depth

Enhance threat efficacy

- World-class security controls

Streamline security management

- Consolidate security to share threat intelligence

Stop more threats

- Continuous analysis and retrospective detection

Customers using a competitor's firewall

As your customers continue to add more point products from a pure security vendor, it is inevitable that they will end up with gaps. Cisco's security portfolio provides an unmatched breadth and depth of integrated products, closing these gaps. Further, these solutions work together to share threat intelligence, helping customers improve their overall security posture.

Branch Office

Palo Alto: PA-220/820/850

Fortinet: FG/FWF-30E/50E/60E

Check Point: SG-3100/3200

Small Enterprise

Palo Alto: PA-3220/3250/3260

Fortinet: FG-80E/100E/100F

Check Point: SG-5100/5200/5400

Mid-Large Enterprise

Palo Alto: PA-5220/5250/5260

Fortinet: FG-200E/300E/400E

Check Point: SG-5600/5800/5900

Service Provider

Palo Alto: PA-5280/7050/7080

Fortinet: FG-1200D/1500D/2000E

Check Point: SG-23500/23900

Cisco Security Platform

Messaging to open a conversation with your customer

Turn your entire network into an extension of security architecture

- Leverage Cisco hardware for automated threat detection and response across network architecture
- Integrate routers, switches, SD-WAN, and other Cisco network devices with your firewall
- Protect users, apps, devices, and data wherever they are

World-class security controls

- Protect against emerging threats with leading threat efficacy
- Complete portfolio of NGFW solutions for organizations of all sizes
- Industry-leading threat intelligence and research (Talos)

Unified policy and threat visibility

- Streamline security policy and network device management
- Control and harmonize policy across your extended network
- Accelerate key security operations such as detection, investigation, and remediation

The Cisco next-generation firewall portfolio allows you to protect your workloads from an increasingly complex set of threats while delivering consistent security policies, visibility, and improved threat response. From your data center, branch offices, cloud environments, and everywhere in between, you can leverage the power of Cisco to turn your existing network infrastructure into an extension of your firewall solution, leading to evolved security everywhere you need it. By purchasing a Cisco appliance today, you will be setting the foundation for consistent visibility, policy harmonization, and unified management. Cisco Threat Response automates integrations across the entire Cisco security portfolio so you can rapidly detect, investigate and remediate threats.

Cisco Security Platform

Turn your entire network into an extension of security architecture

Value statement

Trust the network security from the world leader in enterprise networking, providing the deepest set of integrations between core networking functions and network security. Cisco switches and routers can act as security devices, tying existing network infrastructure into your security policies.

Talking points

- Get more from your existing network: Enhance security with existing investments, including Cisco Application-Centric Infrastructure (ACI) and Identity Services Engine (ISE).
- Share threat intelligence: Extend protection across the architecture quickly, helping you correlate seemingly disconnected events, eliminate noise, and stop threats faster.
- Greater security control points: Enforce polices across your entire environment, including nearly any network or security device administered by the organization.

Cisco Security Platform

World-class security controls

Value statement

Protect your network against an increasingly complex set of threats with a complete portfolio of NGFW appliances deployed wherever you need them —across data centers, and multiple clouds.

Talking points

- Stop more threats: Cisco® Advanced Malware Protection (AMP) and Threat Grid detect, and block known and unknown malware.
- Prioritize threats: Gain superior visibility into your environment with Cisco Firepower next-gen IPS. Automated risk rankings and impact flags identify priorities for your team.
- Detect earlier, act faster: Talos research teams collect threat information and deliver protection against attacks.
- Cisco Threat Response: Automated threat response based on intelligence from Cisco Talos. Reacts to new cyberattacks by automatically sharing and deploying countermeasures across the security architecture to cut the time required for detection, investigation, and remediation.
- Protect against hidden threats: Cisco NGFW leverages dedicated hardware to inspect threats hidden in encrypted traffic while maintaining optimal performance.

Cisco Security Platform

Unified policy and threat visibility

Value statement

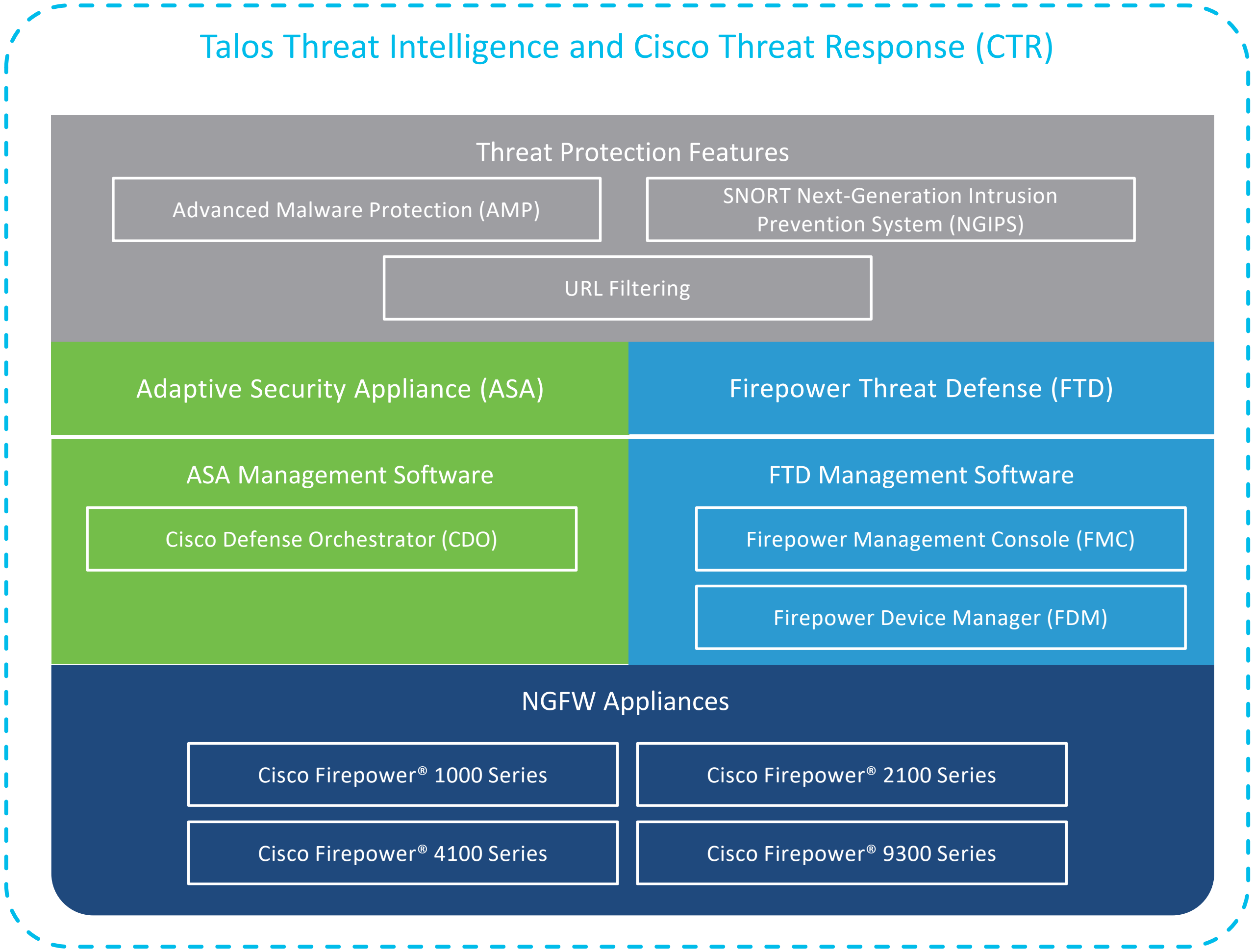
By investing in Cisco NGFW today, you will not only be gaining a stronger security posture but setting yourself up with a future-ready management experience that can evolve with your network.

Talking points

- Cloud management solution: Cisco Defense Orchestrator (CDO) delivers policy harmonization across a variety of Cisco security products.
- Deliver scalable controls across many devices quickly: Leverage CDO for change tracking and roll backs. Harmonize policy and enforcement across thousands of security controls across the network.
- Reduce complexity: Deliver simplicity with unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP.
- Stay ahead of threats: Gain granular visibility of your infrastructure and quickly identify and remediate vulnerabilities.
- Accelerate security operations: Improve efficiency by removing manual processes. With Cisco, you can access security patches and new features faster by completing software image upgrades in a just a few clicks.

Cisco Security Portfolio

Components that make up the Cisco NGFW solution



Talos Threat Intelligence and Cisco Threat Response (CTR)

Threat Protection Features

- Advanced Malware Protection (AMP)
- SNORT Next-Generation Intrusion Prevention System (NGIPS)
- URL Filtering

Adaptive Security Appliance (ASA)

Firepower Threat Defense (FTD)

ASA Management Software

- Cisco Defense Orchestrator (CDO)

FTD Management Software

- Firepower Management Console (FMC)
- Firepower Device Manager (FDM)

NGFW Appliances

- Cisco Firepower® 1000 Series
- Cisco Firepower® 2100 Series
- Cisco Firepower® 4100 Series
- Cisco Firepower® 9300 Series

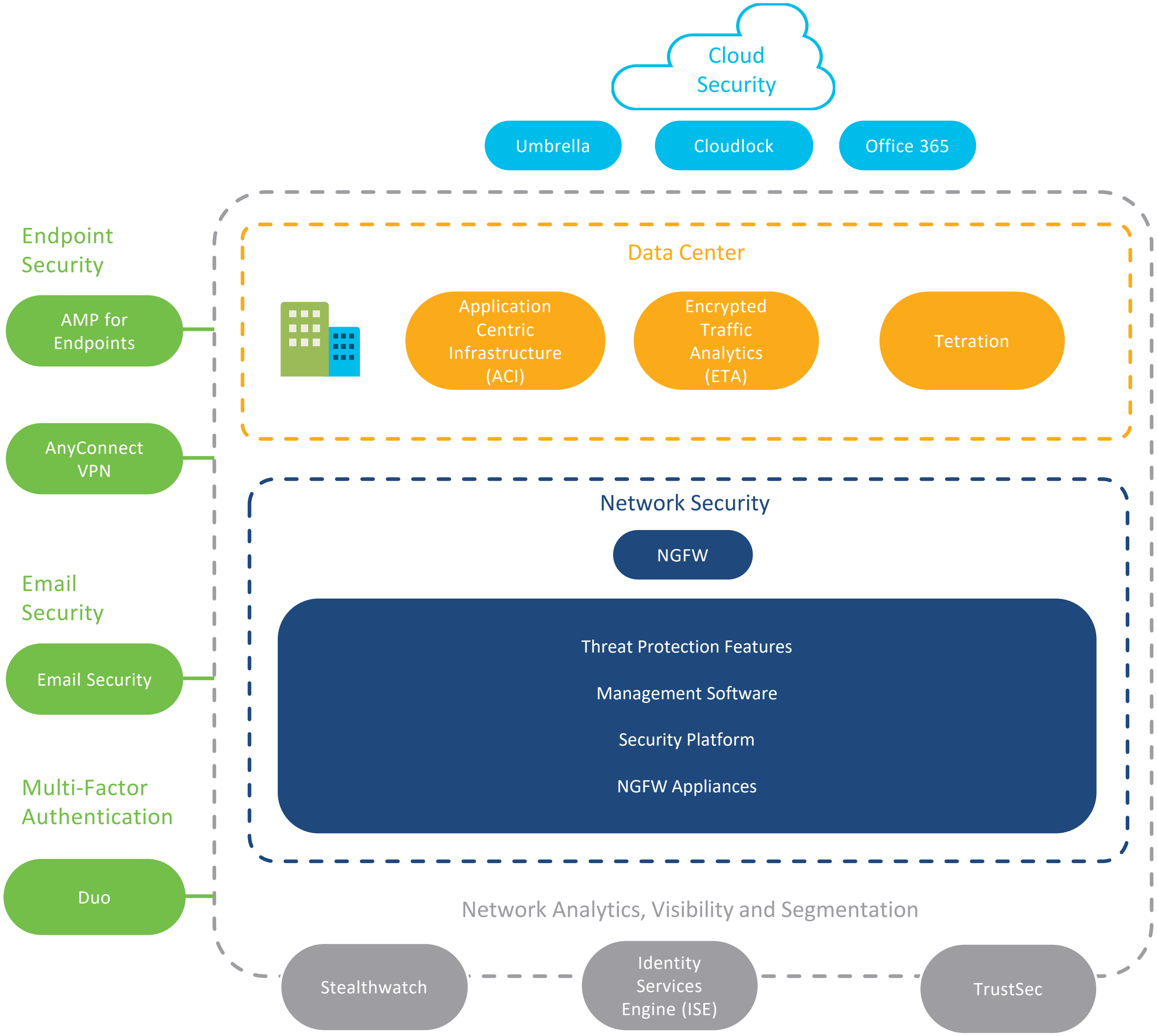
Security product details in Appendix

Start with a Cisco NGFW Appliance

Features	Cisco Firepower® 1000 Series	Cisco Firepower® 2100 Series	Cisco Firepower® 4100 Series	Cisco Firepower® 9300 Series
Hardware Model	FPR-1010* FPR-1120** FPR-1140** FPR-1150***	FPR-2110 FPR-2120 FPR-2130 FPR-2140	FPR-4115 FPR-4125 FPR-4145	FPR-9300 SM-40 FPR-9300 SM-48 FPR-9300 SM-56
Firewall	650Mbps 1.5Gbps 2.2Gbps 3.0Gbps	3Gbps 6Gbps 10Gbps 20Gbps	80Gbps	80Gbps
NGFW	650Mbps 1.5Gbps 2.2Gbps 3.0Gbps	2.3Gbps 3Gbps 5Gbps 9Gbps	26Gbps 35Gbps 45Gbps	48Gbps 55Gbps 64Gbps
NGIPS	650Mbps 1.5Gbps 2.2Gbps 3.0Gbps	2.3Gbps 3Gbps 5Gbps 9Gbps	27Gbps 40Gbps 53Gbps	54Gbps 64Gbps 70Gbps
Transport Layer Security (TLS)	150Mbps 700Mbps 1Gbps 1.4Gbps	365Mbps 475Mbps 735Mbps 1.4Gbps	6.5Gbps 15Gbps 10Gbps	10Gbps 11Gbps 12Gbps
Interfaces	8x RJ45* 8x RJ45, 4x SFP** 8x RJ45, 2GB SFP***	12x RJ45, 4x SFP	8x SFP+	8x SFP+
Optional Interfaces	8x RJ45, 2x10GB SFP***	10G SFP+, 1/10G FTW	2x NM's: 1/10/40G, FTW	2x NM's: 1/10/40/100G, FTW
Use Cases	Small Business, Home Office, Branch Office, Small/Mid Enterprise	Mid/Large Enterprises, Internet Edge, Data Centers	Data Centers, Internet Edge	Service Providers, Data Centers, Campuses, High-Performance Computing

Add additional security products for an integrated security portfolio

Up-sell to protect your customer's entire enterprise. Talos Threat Intelligence and Cisco Threat Response (CTR) are included in every appliance and product that Cisco offers.



Security product details in Appendix

How to identify new opportunities

Prospecting

LinkedIn Titles keywords – SecOps, NetOps, CISO, Security Taskforce, Security Professional/Officer/ Engineer/Analyst, Cloud Taskforce

LinkedIn Groups – Cloud Computing, The Virtualization & Cloud Computing Group, Virtualization & Cloud Computing Solutions, Information Security Community, Information Security Network, Security Industry Group, Group Security Alliance, Security Experts – A Global Group, Security Specialist, IT Security Group

Understand Customer Business Drivers

- Digital transformation projects
- Efforts to modernize IT operations
- Board of Directors mandating security risk report
- Projects that expand the enforcement point, such as new cloud apps, IoT, branch office, remote employees, vendor portals, or mobile devices

Key questions to assess customer needs

1. What is your current firewall strategy for your: internet edge, remote locations, cloud environments, data center?
2. Are you facing performance issues with your current firewall appliances when using multiple security features, inspecting encrypted traffic, IPS or logging and NAT are enabled?
3. Do your existing security products work together to share threat intelligence?
4. Are your existing NGFW solutions and other security products tightly integrated with your routers, switches, and other network devices?

Target Audience

- Learn about their IT current and future projects
- Use key questions to identify the challenges that prevent them from reaching their IT goals
- Listen for triggers within your accounts for opportunities to discuss the benefits of NGFWv

New Opportunities

Firewall discussions create opportunities to either upgrade existing customers to NGFW or displace competitor firewalls.

Engage C-level and executives in security discussions to penetrate your accounts for further business opportunities.

Discuss future-proofing with next-generation technology to ensure your accounts are secure as their IT landscape shifts.

Look for these triggers

- Security breach
- Digital transformation (DX)
- ERP apps moving to cloud
- Hybrid cloud infrastructure
- Remote users, contractors, and third parties
- IoT devices
- Global expansion

Personas

CISO

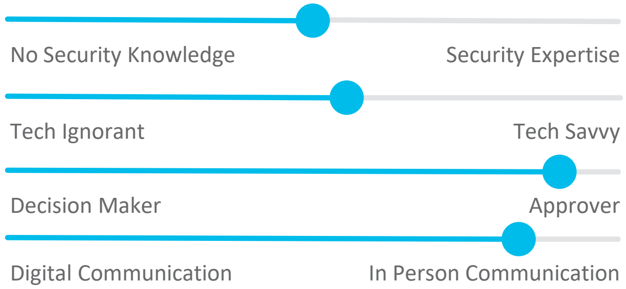
Decision Maker

> “I’m responsible for the protection of our enterprise information assets and technology and executing our security programs.”

Responsibilities

Executive responsible for the overall security strategy direction, operations, and the budget for the protection of enterprise information assets and manages that program.

Insights



Challenges

- A lot of attention on growing data breaches and falls on their shoulders
- Disparate security solutions and limited visibility across enterprise
- Meeting compliance demands
- Difficult to hire security talent
- Moving workloads to cloud
- Lack of talent and budget to manage all point security products

Priorities

- Setting organizational security strategy
- Mitigate risk
- Application performance and security
- Complying with regulatory mandates
- Safeguarding customer data and protecting the brand of the firm
- Manage and train security staff with the right tools
- Security risk report for Board of Directors

Listen for

- Interest in automating security operations to save time and reduce complexity
- Looking to increase security visibility across network to improve threat detection and reduce remediation time
- New projects that will expand the enforcement points, such as cloud applications, new SaaS apps, IoT, branch offices, customer portals

Personas

Network Operations Administrator

Influencer

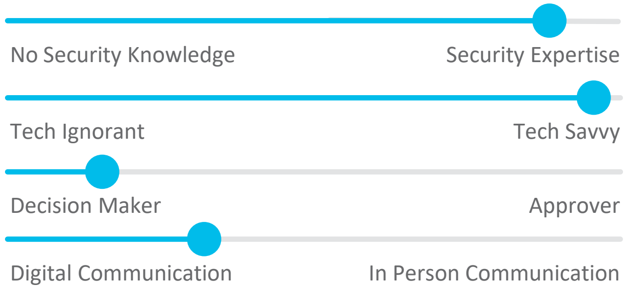
“I’m responsible for the day-to-day operations
of our network and
oversee security.”

Responsibilities

Manage IT infrastructure and provide technical input on future technology direction for the organization.

Security responsibilities may overlap with a System Administrators title, or Security Administrator.

Insights



Challenges

- Interrupt relevant security alarms to uncover actional intelligence
- Cloud projects provisioned, and deployed within 24 hours and often launched without a security strategy
- Intrusion prevention is more difficult as cybercriminals use machine learning to exploit vulnerabilities
- Resource constrained, and lack of skilled security professionals

Priorities

- Monitor security alarms and parse through logs and data to proactively manage threats
- Keeping data, apps, devices, and networks secure
- Ensuring the network is available, performant, reliable, secure, and compliant
- Contribute to the business cases for technology investments

Listen for

- Decentralized policy management with limited visibility to security across network
- Inability to share threat intelligence across enterprise
- Using multiple security vendors
- Upcoming merger activity
- Data center lease expiry
- Challenges managing heterogeneous network
- Projects that expand threat landscape such as deploying new applications, IoT and workloads into the cloud

Personas

Systems Administrator

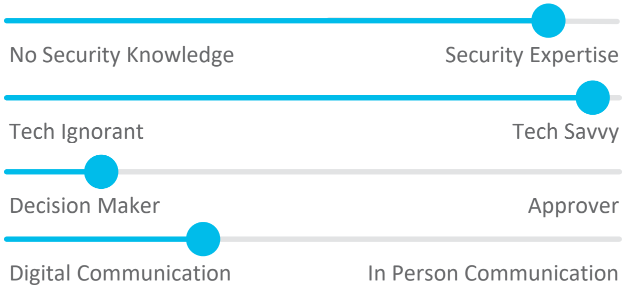
Influencer

"I manage our computing resources on-premise and cloud, which includes servers and desktops, and the services and application that run on them."

Responsibilities

Installing OS and software updates, executing backup and recovery operations, managing authentication systems like Active Directory, and maintaining servers.

Insights



Challenges

- Maintain consistent policy across network environments
- Staying on top of the latest promising technologies
- Difficulty managing complex network
- Evolving security and threat landscape
- Maintaining compliance with regulatory requirements across the enterprise
- Expanding Shadow IT usage

Priorities

- Define security policy across devices
- Ensuring OS and software updates are current for all on-prem devices
- Firmware upgrades to all network devices
- Managing virtual machines in the data center and the cloud
- Capacity planning, hardware inventories, and software license tracking

Listen for

- Performance concerns with current firewall appliances
- Opportunities to show proof via case studies
- Any new projects that expand the enforcement point, such as new SaaS applications, cloud applications, branch office, remote employees, vendor portals, mobile devices, or IoT devices

Competitive positioning

Palo Alto Networks Claim	Cisco Response
Panorama Firewall Manager offers simpler policy enforcement, streamlined management and automation, and insights to prevent cyber attacks	Panorama doesn’t have automatic threat containment like FMC. Palo Alto doesn’t allow custom Application or IPS Signatures, or IPS Tuning, and Panorama lacks security analytics. Panorama may have a great interface, but it’s not set and forget.
Cortex XDR enables automatic detection, accelerated investigation, and quick elimination of security threats	Cortex XDR comes at an additional cost and cannot currently perform enforcement. CTR is threat management portal that is included with Cisco firewalls for free.
Highest NGFW on the Gartner Magic Quadrant	Palo Alto worked with Gartner to create the NGFW category, so their placement is largely the result of a perception that they’re the de facto standard. However, security is about much more than the NGFW. PAN lacks tight integrations with other products, has poor threat efficacy, and a less deep portfolio than Cisco.

Competitive positioning

Palo Alto Networks Claim	Cisco Response
Cortex XDR is too new to adequately compete with CTR and comes at an additional cost	CTR has proven track record and comes included without additional fees.
Security portfolio doesn't function as an integrated architecture	Cisco is ideal for businesses looking to consolidate their security architecture with a single vendor. Our integrated portfolio not only delivers more comprehensive security, but operational efficiencies as well.
Is perceived as a leading security company but has poor threat efficacy	Cisco's threat efficacy is better than PAN's. Cisco founded the Cisco Security Technical Alliance with over 150 participatory organizations engaged in threat intelligence automation and sharing.
Palo Alto Networks 'gives away' endpoint protection, detection, and remediation tool, which cannot compete effectively with Cisco's	Lean on the AMP+CTR combination as the best-in class endpoint/ threat investigation combination.
Over-pivots on threat prevention, when detection and remediation are also critical	Our portfolio bundles threat detection, prevention and remediation together, helping customers not only stop, but see and respond to threats. We also offer retrospection, which allows customers to perform more effective analysis of past vulnerabilities and attacks.

Competitive positioning

Fortinet Claim	Cisco Response
Price per protected megabit	Up-level to a broader conversation around the entire portfolio
Specialized dedicated 'in-box' processor technology/ ASICS	Fortinet's performance advantage goes away as soon as advanced features such as IPS and anti-malware are turned on.
Reported high VPN throughput and connectivity. Encrypt/Decrypt is offloaded to ASICs.	VPN throughput measurements are made with all advanced features turned off. Once advanced features are turned on, VPN throughput performance drops noticeably. Challenge Fortinet to provide list of FortiClient customers that actually use their client VPN and ask for a total number of FortiClient customers.
FortiManager is feature rich with similar performance and effectiveness compared to FMC, but a more streamlined management experience	Cisco has flexible management options with CDO and FMC. Greater integration with NGFW capabilities such as CTR, ISE, and AMP4EP.
Fortinet Security Fabric does everything from endpoints to multi-cloud with automation, visibility, and security.	Fortinet Security Fabric requires Fortinet Switches, which are not enterprise-grade. Most businesses choose Cisco or Juniper switches and will not want to use FortiSwitches just for the security fabric.
Ease of deployment in a distributed environment	While Fortinet offers easier deployment of their NGFWs in distributed environments, SMB's need more than just firewalls, they need a complete security architecture. New 1000 series Cisco appliances, when combined with the rest of the portfolio, provide enterprise-grade security for companies of any size.

Competitive positioning

Fortinet Claim	Cisco Response
Depth and breadth/ integration of portfolio	Cisco's integrated portfolio offers integration, threat efficacy, correlation of threat intelligence across entire network nearly instantly after threats are detected. Fortinet's propriety IPS cannot compare to industry-leading SNORT IPS– point out that the Fortinet IPS is not even on Gartner's MQ.
NGIPS capabilities and performance	Fortinet lacks true next-generation IPS capabilities, which is why Fortinet is missing from Gartner's NGIPS Magic Quadrant report. Cisco's SNORT NGIPS is an open source industry-leading solution powered by Talos Threat Intelligence.
FortiGuard Threat Intelligence	Talos Threat Intelligence is rated higher on proactive alerts, malware detection, intelligence reports, endpoint intelligence, and security validation per G2. Talos has a global footprint, collects over a million malware samples a day, and has extensive industry partnerships enabling the latest in threat intelligence, including zero-day threat protection.
Can't perform threat impact analysis without endpoint details, endpoint not designed to integrate with security inputs (Source: Gartner)	Cisco's NGFW appliances are deeply integrated with CTR, AMP4EP, and ISE, providing direct threat containment at every level.
Drill-in forensics per event require FortiSandbox and FortiAnalyzer, which come at an additional cost	Context Explorer included in Cisco FMC with CTR and ThreatGrid included at no additional cost.
No network and endpoint awareness, continuous analysis and retrospective detection, or process/threat trajectory	Cisco AMP and CTR allow for retrospective detection with network and endpoint awareness.
Security Fabric doesn't sell well	Fortinet Security Fabric only shows real value when using Fortinet Switches. Most customers are not running such appliances, nor do they want to. Customers gravitate towards appliance and software bundles.

Competitive positioning

CheckPoint Claim	Cisco Response
Faster and simpler deployment of firewalls	Cisco firewalls may take slightly longer to deploy, but the increased granularity of configuration provided enables more effective network security.
Check Point SandBlast	Remind the customer that Sandblast Sandbox has decent adoption, but that the endpoint and mobile products are not widely deployed and ask them to consider why.
Completeness of security vision	Compared to Cisco, Check Point’s solution is still a series of disparate point security products that cannot match Cisco’s level of cohesiveness and integration.
Largest offering of security solutions	As a traditional firewall company, many of their solutions are perimeter and prevention focused and are not complete. Most organizations need to augment a Check Point solution with solutions from other vendors to build an effective security strategy.
Top-tier security management	Remind the customer that Check Point has strong firewall management, but the management simplicity stops there. From a holistic perspective, managing the entire Cisco security portfolio is simpler than the Check Point alternative. You can also talk about flexibility enabled by having the choice to use multiple management consoles and talk about integrations being added to CDO soon.

Competitive positioning

CheckPoint Claim	Cisco Response
Cost of license renewals goes up significantly every year	Lean on the customer's pain of perpetually increasing costs. IPS, anti-malware, and other advanced solutions are sold in bundles, but then customers must re-subscribe to each one individually. Check Point customers have been known to experience considerable sticker shock during renewal time due to substantial price increases.
Cannot perform threat impact analysis or prioritize investigations without endpoint details. Endpoint is not integrated with threat emulation or security inputs	IPS Impact flags allow customers to very quickly understand the potential implications of a threat and prioritize accordingly.
Doesn't provide active remediation on Endpoint, client vulnerability management, or incident control and response tools	Full integration of endpoint security via AMP4EP into CTR. Endpoint detection informs CTR which updates across Cisco security architecture. Strong integration with SIEM solutions including Splunk and IBM.
NGFW price per performance is not competitive	Cisco consistently out-performs Check Point during price/ performance comparisons.
Poor threat efficacy	Cisco firewalls offer industry-leading threat efficacy, allowing customers to defend against threats that would go undetected by Check Point NFGW solutions.

Objection handling

Objection	Response
Everything is working fine. Why should I change?	• A large part of operating successfully in the digital age is staying ahead of threats. With Talos you have a security team of 600+ experts working day and night to ensure that your security posture is ready for the most current threats today and tomorrow. • Threats are becoming more sophisticated and more impactful with each passing year. You need a portfolio of security appliances that are flexible and resilient to scale with your business, no matter where your workers are deployed across the globe and in any environment, from cloud, hybrid cloud, and on premises Cisco NGFW covers your assets. • For existing Cisco security customers, upgrading your appliance today gives you a 3.5x performance boost in NGFW throughput, up to 2x more connections per second, and up to 3x performance boost for encrypted traffic compared to prior generation appliances. More importantly, you will be setting the foundation for consistent visibility, policy harmonization, and improved threat response.

Objection	Response
We're concerned about a lack of unified firewall management solutions.	Customers have the flexibility to use a variety of Cisco management platforms like Cisco Firepower® Management Center (FMC) and CDO. CDO currently works with Firepower and ASA appliances and Meraki, and we're aggressively adding additional integrations with CDO. Eventually, you will be able to manage all your Cisco security devices through one single interface with CDO.

Objection	Response
Cisco has overly-complex management of firewalls.	We want our customers to have the flexibility to choose the management that works for them, so we offer FMC, FDM, and CDO. In the near future, we will continue to add new integrations with CDO, helping you consolidate security management into one interface.

Objection handling

Objection	Response
We lack in-house IT staff. I need a simpler network solution.	• Cisco Firepower enabled appliances can be centrally managed by Cisco Firepower Management Center (FMC), which provides clear network visibility with policy automation that responds to the changing threat landscape. This capability correlates detailed network and endpoint event information and provides further visibility into malware infections. • CDO will simplify management across your entire security and network architecture. Multiple management consoles will not be necessary, therefore smaller teams can manage a global corporate network. • If you need a simpler network solution, you need a simpler security solution. Cisco's integrated, end-to-end security architecture reduces the complexity that comes with trying to stitch together bunch of point security products. An integrated architecture provides operational efficiency built on automation and orchestration, allowing for smaller teams to be more effective.

Objection	Response
We would prefer to go with a security vendor, since Cisco is all about networking.	Cisco is the largest security vendor in the industry with a comprehensive portfolio of leading products and solutions designed to help customers defend their networks, users, data and workloads from even the most sophisticated threats. With Cisco you can also leverage your investment in infrastructure to turn your entire network into an extension of your security architecture. When it comes to integrated network security, no one can match our level of integration with every device on the network, including routers, switches, gateways, SD-WAN solutions, intent-based routing, and more. We understand the intricacies of enterprise networks, which makes us uniquely positioned to secure those networks. Pure play security vendors are not able to deliver the same level of integration we can.

Challenger Selling Model

Cloud

Message target

CISO, Network Operations Administrator, and Security Operations Manager

Customer challenge summary

Migrating network resources to the cloud and extending policy to minimize risk exposure

Cisco solution summary

- Reduce complexity with unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP
- Gain more insight with Cisco Firepower® NGFW for visibility into your environment with next-gen IPS

Challenger Selling Model

1. Warm up: Cloud computing is being adopted at an unprecedented pace, and forecasts indicate that 41% of all enterprise workloads platforms by 2020. Adding to the complexity, Shadow IT is 30 to 40% of IT spending in large enterprises. Securing the cloud is difficult without comprehensive visibility, policy consistency, automation, and the ability to share threat intelligence.
2. Reframe: The security of the cloud is complex with sensitive data accessed through virtual machines and demands for regulatory compliance leading to more point security solutions. The average enterprise has 75 security tools , and 82% of companies want an integrated security portfolio. Multiple point security solutions hinder visibility across the entire enterprise and is a burden on IT.
3. Rational drowning: Your IT is managing security with multiple vendors and configuring thousands of cloud resources individually. Complexity leads to misconfiguration that increases the risk for a security breach. Through 2025, at least 99% of cloud security failures, and 64% of organizations said that human error was the main cause of misconfiguration. Cybercrime damages are real and will cost the world $6 trillion annually by 2021.
4. Emotional impact: Cloud security misconfiguration opens the door for cybercriminals, who use scripted attacks to access sensitive data. Imagine the aftermath of a security breach if thousands of your customers' social security numbers are compromised.
5. A new way: Using an integrated security architecture, with a modern NGFW at its core, improves security posture in the cloud by reducing configuration errors with automation and visibility into duplicate and shadow policies. Advanced threat intelligence can evaluate and prioritize threats with detailed impact flags across the network using automation.
6. Your solution: Cisco Firepower® NGFW offer a new approach with an integrated architecture and advanced threat protections to minimize configuration errors.

Challenger Selling Model

Internet Edge

Message target

Network Operations Administrators, and System Administrators

Customer challenge summary

Protect your business against threats hidden in encrypted traffic while providing the performance and high availability that your end users and stakeholders expect.

Cisco solution summary

- Threat intelligence integrated across Cisco Firewall, AMP for network and AMP for Endpoint can block HTML type attacks
- The visibility of Firepower Management Center (FMC) blocks malware and encrypted traffic while delivering performance and high availability to meet demanding SLAs

Challenger Selling Model

1. Warm Up: The internet edge is the network infrastructure that provides connectivity to the Internet, and that acts as the access point for the enterprise to the rest of cyberspace. Protecting the internet edge against attacks hidden in encrypted traffic is more challenging. Plus encrypted traffic is rising fast. 94% of all Google web traffic is encrypted. While encryption safeguards data, hackers are using encryption for their attacks, making it harder to find malicious threats.
2. Reframe: The internet edge plays a critical role in supporting the services and activities that are fundamental to the operation of the modern enterprise. As demands for your business grows, so does the capacity to scale, provide high performance to your end-users, and protect against threats. Detecting malicious network traffic hidden within encryption consumes a lot of firewall processing and can negatively impact the speed for everyday business requirements.
3. Rational drowning: Gartner believes that by 2020, more than organizations will fail to decrypt HTTPS traffic efficiently, "missing most targeted web malware." A typical $3.86M, and malicious or criminal attacks initiate 48% of all breaches. According to NSS Labs, very few security devices can inspect encrypted data without severely impacting network performance. On average, the performance hit for deep packet inspection is 60%.
4. Emotional impact: Most organizations don't have a solution to detect malicious content in encrypted traffic, but let's say you do. The industry average detection time for a breach is 197 days. In less than 30 days, a large-scale cyberattack can highjack banking data from 40 million customers and personal data of another 70 million customers. In minutes, the data is resold on the black market and customer personal information, and bank accounts exposed.
5. A new way: World-class security controls detect and block more sophisticated threats. Granular application control can protect against malware and gain full contextual threat analysis, while hardware decrypt offload improves the performance of encrypted traffic in the data center. Integrated portfolios have threat intelligence that backs all network devices to keep your organization safer while delivering superior performance and high availability.
6. Your solution: Cisco Firepower® NGFW offers intelligent threat context, dynamic, flexible controls, multi-layered threat detection and mitigation with hardware decrypt offload to improves encrypted traffic performance and provide high availability.

Challenger Selling Model

Data Center

Message target

Network Operations Administrator, and System Administrators

Customer challenge summary

Logically group data center resources and apply security policies throughout to protect against malicious
insider attacks

Cisco solution summary

- Microsegmentation with Cisco ACI
- Gain insights into and control over threats and vulnerabilities across cloud, network and endpoints
- Threat focused to provide granular application control to protect against malware
- Shrink time to detection and mediation

Challenger Selling Model

1. Warm Up: The data center houses your applications and most business-critical data. Organizations are using server virtualization to scale and leverage hardware resources. According to Cisco's Global Cloud Index, 76% of the traffic is between VMs and applications, never leaving the data center.
2. Reframe: Security teams focus on the "North-South" traffic that enters and exits the data center when the majority of the traffic is "East-West". The Verizon 2019 Data Breach Investigations report says that 34% of all breaches in 2018 were caused by insiders. Accenture & Ponemon's 2019 Cost of Cybercrime study states the average cost of a malicious insider attack rose 15% from 2018 to 2019 and insider-related incidents can cost a company up to $8.76 million a year.
3. Rational drowning: According to Ponemon, the average cost of an insider-related incident is around $513,000. With so many devices accessing the data center, threats enter the organization via email, collaboration tools, and mobile devices spreading within a data center rapidly if the internal network is not protected. Threats can propagate the network, quickly and jeopardize business operations without complete network and end point visibility.
4. Emotional impact: Securing the perimeter does not protect against insider attacks. A new vendor portal was launched, facilitating self-service with access via mobile devices. Within months, a compromised mobile device introduced malware when accessing internal data leading to a cyberattack. Sensitive customer data was accessed. The firm lost their five top customers, and the executive team is launching costly campaigns to restore customer confidence.
5. A new way: Using a security solution that provides complete network visibility, IT can maintain consistent policies and stay ahead of threats with in-depth visibility to the endpoints. Comprehensive and unified management over firewalls, application control, intrusion prevention, inter-VM traffic, URL filtering, and advanced malware protection, ensures your internet edge is protected.
6. Your solution: Cisco Firepower® NGFW offer a broad portfolio to protect the data center with comprehensive visibility to see traffic between VMs, applications and physical servers, and detects attacks earlier and block threats faster.

Challenger Selling Model

Small Business/Branch

Message target

Network Operations Administrator, and System Administrators

Customer challenge summary

Protect their business with enterprise level security that is affordable

Cisco solution summary

- Simpler management experience
- Incident response provides faster time to protect and remediate attacks
- Gain insights into and control over threats and vulnerabilities across cloud, network and endpoints

Challenger Selling Model

1. Warm Up: Cybersecurity is not just a problem for larger organizations. Small business remains a target for a substantial number of malicious attacks. They are hit by 62% of all cyberattacks, about 4,000 per day. So, when the network is down, your business is effectively down too.
2. Reframe: Small businesses often do not invest in enterprise grade security since they don't have the IT resources to manage complex security solutions. Thus, threats hit a user's email inbox using spam and phishing or identify vulnerabilities on computers and run malicious code to exploit. Small businesses need to protect their business against these growing threats.
3. Rational drowning: Operations within a small business use multiple access points - mobile devices, cloud applications, and contractors all accessing the network. These points of access increase the attack surface and put the business at risk for malicious activities. The average cyberattack cost to a small business is $86,500.
4. Emotional impact: Imagine your manufacturing line processing your biggest order just as your fleet manager is redirected to a malicious web site. Within minutes your back-office application halts. IT scans the antivirus software, but it doesn't identify the threat delaying your largest customer order.
5. A new way: The best way to prevent a cyberattack is to ensure your business has the protection it needs to stay ahead of threats. With easy to use management software, you can protect against advanced threats with application visibility and control to detect and stop threats fast. Secure and protect your traffic against hidden threats, advanced malware protection, and URL filtering.
6. Your solution: Cisco Firepower® NGFW provides optimal price and performance with application visibility and control, advanced malware protection, and URL filtering. Built-in automation simplifies security management for small businesses and branch offices providing the best security, performance and price.

How to Buy

Cisco Commerce is the primary tool used for registering opportunities and ordering Cisco products and services on the Cisco Price List. Three main steps are involved in creating an order:

1. Creating a quick quote
2. Converting a quote to an order
3. Submitting an order

Steps to get started:

1. Identify your customer's installation base (ASA installation base)
2. Identify key objectives, strategy, and needs
3. Apply that to the ASA Migration Template
4. Take advantage of discounts
5. Register opportunities in Cisco Commerce
6. See step-by-step instructions for the Security Competitive Refresh Registration Process
7. Eligible products will receive those discounts
8. After an opportunity has been approved, you may offer your quote to a customer

Cisco Commerce

Partners can order Cisco products easily using Cisco Commerce using a few easy steps.

1. Select the primary bundle part numbers and software image
2. Choose Subscriptions
   - Type and Term (1, 3, or 5 years)
3. Select Base Software License for each security module
4. Save and exit

Smart Licensing

Smart Licensing is Cisco's new licensing system. It enables customers to easily move licenses themselves between similar systems in their organization, overcoming limitations associated with previous device-locked Product Authorization Key (PAK)-based licenses. Become familiar with the new Smart Software Licensing portion of the ordering process.

Enterprise Agreements

The Cisco Enterprise Agreement is a 3- or 5-year agreement that provides enterprise-wide coverage of software enrollments for an easier software management experience than alternative buying programs.

Resources

Partner Specific Resources

For more guidance on how to position and sell Cisco NGFW, check out the following Partner resources on SalesConnect.

- Partner call script: This call script will help you describe the value of Cisco NGFW and walk through typical customer scenarios that could lead to opportunities.
- Partner Sales Sheet: This will help sellers pitch the Cisco NGFW value proposition to customers and prospects and walk them through the sales process and Cisco NGFW offerings
- Co-branded Partner sales kits
  - Business Development Manger deck
  - Technical Development Manger

Additional Resources

You can learn more about the Cisco NGFW portfolio by accessing additional resources on Cisco SalesConnect. There you will find:

- Battlecards: Walk through competing with Fortinet, Palo Alto, and Check Point
- Sales Briefs: Provide extensive information on selling our portfolio successfully
- Spec Sheets: Cisco NGFW hardware infused with differentiation messaging
- Interactive eBook: Explore each use case in our interactive eBook that is publicly available
- Additional public-facing assets are available, including pitch decks, product-at-a-glance documents, solution overviews, and more

Cisco SalesConnect

Learn more about the Cisco NGFW security portfolio by visiting the NGFW page on Cisco SalesConnect.

Customer Success

"Security is no longer a second consideration for us… it's an assumed part of everything we do, This ELA is an integrated set of tools that allows my existing team to meet our larger mission: transformed digital learning."

Drew Lane
Executive Director of ICT
Shawnee Mission School District

Challenges

- Securely implement digital initiative to provide mobile devices for students and teachers
- Fragmented infrastructure hindered progress and posed a security risk

Solutions

- Cisco Firepower 9300 Security Appliance
- Cisco Collaboration Enterprise License Agreement

Results

- Decreased the number of malware incidents from three per day to one per month
- Improved productivity and collaboration among students and teachers

Customer Success

"We can write sets of rules that apply across the entire network, rather than focusing on individual devices, saving us an enormous amount of time. It gives us peace of mind knowing that we're stopping a lot of that stuff that we believe used to come through our environment."

Wes Dawes
Senior Network Administrator
SugarCreek

Challenges

- Using Cisco ASA 5545, a legacy security system
- Manufacturing techniques changing and their network is being accessed by more vendors increasing their security risk

Solutions

- 18 Cisco Firepower 2110 NGFW (HA pairs) with Firepower Threat Defense
- AMP for Endpoints
- AnyConnect VPN

Results

- Security definitions are automatically updated and pushed out through AMP for network and endpoints protecting against new vendors coming online
- Visibility across the network to monitor and pool all threat intelligence in one place to isolate threats before they become widespread

Appendix

Integrated Security Portfolio

Platform

Adaptive Security Appliance (ASA) Family of security devices including industry-recognized stateful firewalls. Delivers enterprise-class firewall capabilities in an array of form factors —standalone appliances, blades, and virtual appliances —for any distributed network environment. Delivers comprehensive solutions that meet continuously evolving security needs.

Cisco NGFW (Firepower & FTD) Integrated suite of industry-recognized stateful firewalls, network security, traffic management products, and NGFW deployed either on purpose-built platforms or as a software solution. Designed to permit and deny network traffic in compliance with an organization's security policy.

Management Software

Cisco Defense Orchestrator (CDO) Helps consistently management policies across Cisco security products. Cloud-based application simplifies management, improves efficiency, and strengthens security.

Firepower Management Console (FMC) Administrative nerve center for management of critical Cisco network security solutions. Provides unified management over firewalls, application control, IPS, URL filtering and AMP.

Firepower Device Manager (FDM) On-box management console that can be accessed via an internet browser. Enables fast deployment, policy customization, reporting, and management of firewall appliances.

Threat Protection

Talos Threat Intelligence 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 unmatched visibility into the latest global threats, actionable intelligence on defense and mitigation, and collective response to ensure all Cisco customers are actively protected.

Cisco Threat Response (CTR) Automated threat response based on intelligence from Cisco Talos. Reacts to new cyberattacks by automatically sharing and deploying countermeasures across the security architecture. Dramatically cuts the time required for detection, investigation, and remediation.

Advanced Malware Protection (AMP) Global threat intelligence, advanced sandboxing, real-time malware blocking. Continuously analyses file activity across extended network for quick detection, containment and removal of advanced malware.

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

URL Filtering To control the websites that users on your network can access. Enforce policies on hundreds of millions of URLs in more than 80 categories.

Cloud Security

Umbrella Uses the internet's infrastructure to block malicious destinations before a connection is ever established. Learns from internet activity to automatically identify attacker infrastructure staged for current and emergent threats. Umbrella captures and understands relationships between malware, domain, IPs, and networks across the internet.

Cloudlock Cloud-native cloud access security broker (CASB) which helps migrate data to the cloud safely. Protects cloud users, data, and apps with a simple, open, and automated approach using APIs to manage risks in cloud app ecosystems. Easily combat data breaches while meeting regulatory requirements.

Office 365 Identify threats faster and remove them automatically from Office 365 inboxes.

Data Center

Application Centric Infrastructure (ACI) Facilitates application agility and data center automation with a consistent policy model. Can move apps seamlessly to any location or cloud while maintaining security and high availability.

Encrypted Traffic Analytics (ETA) Enables enhanced visibility and insights into threats in encrypted traffic without the need for decryption. Uses network analytics and machine learning to shorten response times in containing infected devices and users. Promotes compliance with cryptographic protocols.

Tetration Offers holistic workload protection for multi-cloud data centers by enabling a zero-trust model using segmentation. Allows identification of security incidents faster, contains lateral movement, and reduces attack surface through an infrastructure-agnostic approach both on-premises and in the cloud

Network Analytics, Visibility and Segmentation

Stealthwatch Outsmart emerging threats with industry-leading machine learning and behavioral modeling. Know who is on the network and what they're doing using network infrastructure telemetry. Detect advanced threats and respond quickly. Protect critical data with smarter network segmentation.

Identity Services Engine (ISE) Offers a network-based approach for adaptable, trusted access everywhere, based on context. Provides intelligent, integrated protection through intent-based policy and compliance solutions. Delivered via streamlined, centralized management that enables secure scaling.

TrustSec Software-defined segmentation to apply policies across the network in scale. Use ISE to manage TrustSec security group tags and share information with other group-based policy schemes.

EndPoint Security

Advanced Malware Protection For Endpoints (AMP4EP) Prevent threats at the point of entry, then continuously track every file it lets onto your endpoints. AMP4EP can uncover even the most advanced threats, including file-less malware and ransomware —in hours, not days or moths.

Cisco AnyConnect Cisco's VPN and Access platform that simplifies secure endpoint access and provides the necessary security to help keep your organization safe and protected.

Email Security

AMP for Email AMP analyzes emails for threats such as zero-day exploits hidden in malicious attachments. It gives you advanced protection against spear phishing, ransomware, and other sophisticated attacks.

Multi-Factor Authentication

Duo Provides multi-factor authentication, endpoint visibility, adaptive authentication and policy enforcement, and remote access and single sign-on.