Cisco Next Generation Firewalls

Partner Call Script

Call Script Guide:

When the caller speaks: Text is black

When the call recipient speaks: (Text is in parenthesis)

[Variables will be blue and in brackets] and the caller should decide which path to follow

When general instructions are given: **Text is bold**

Call Introduction:

Hi, this is _____, from [Partner Name]

The two options presented here are meant to differentiate existing Cisco customers from non-Cisco customers.

[Existing Cisco Customers Prompt]: The reason for my call is that you are an existing Cisco firewall customer, and we wanted to talk about how upgrading your Cisco firewall will protect your business against not only the latest threats today but will keep you ready for the evolving threats of tomorrow.

Do you have a few minutes to talk?

[Non-Cisco Customers Prompt]: The reason for my call is that the traditional all-encompassing single-firewall approach is no longer adequate for modern business environments. Multiple micro-perimeters are needed from the data center to the mobile endpoint, and I'd like to discuss how Cisco's Firepower Next-Generation Firewalls can provide your business with the flexibility and threat efficacy needed in today's landscape.

Do you have a few minutes to talk?

Wait for call recipient to respond.

[NO] (The call recipient responds negatively) Is there a better time to call you back? I'd love to tell you about Cisco's NGFW portfolio and the suite of products that will keep your business' network protected from the future of evolving threats.

[YES] (The call recipient responds positively) Great! I wanted to walk through some of the reasons the Cisco NGFW appliances might be right for you:

If the caller is an existing Cisco customer, ask if they are an ASA customer looking to upgrade their ASA appliance or an ASA customer looking to migrate to a NGFW. Depending on response, use one of the "Existing" prompts.

[Non-Cisco Customers Prompt] Cisco NGFW solutions provide consistent policy and visibility, world class security controls, and can turn your existing network into an extension of security architecture. Which of these areas jumps out to you as an area of interest for your organization?

Wait for call recipient to respond.

That's great, based on the size of your business I wanted to walk through which specific appliance can help your organization and how it can hopefully address your needs.

Follow up with scale of networking question.

[Existing Cisco ASA Customers Needing to Upgrade to a Newer ASA Appliance] For existing Cisco ASA customers, you will gain more performance and plenty of overhead capacity.

[Existing Cisco ASA Customers Looking to Upgrade to a NGFW] If you are looking to upgrade to a NGFW, your installed Cisco appliances, routers, and switches can immediately become integrated enforcement points. I would love to know more about your business-

Follow up with scale of networking question on the next page.

Could you inform me what scale of networking and security operations your organization operates at?

Wait for Response

(Call recipient responds with a description of their organization's scale and networking/security operations) Choose a response from below based on the approximate size of their organization.

[SOHO / SMB / Remote Office / Branch Office / Mid-size]
The Cisco Firepower 1000 series appliances would be a perfect upgrade to gain NGFW capabilities for your sized organization. Gain site-to-site VPN, Application Visibility and Control, Dual-WAN, and Advanced Malware Protection capabilities across your entire network with just one Cisco appliance.

[Existing Cisco ASA Customers]: If you are an ASA customer, you can gain Application Visibility and Control, Dual-WAN, and Advanced Malware Protection capabilities across your entire network with just one Cisco appliance.

[Large Size / Enterprise]
The Cisco Firepower 2000 series appliances would be a great fit for your organization's NGFW needs. By upgrading, you'll be able to leverage Cisco Threat Response and Snort NGIPS powered by Talos Threat Intelligence. You'll have the latest threat telemetry powering automated response systems to keep your networks secure.

[Existing Cisco ASA Customers]: If you are an ASA customer, you can gain Cisco Threat Response and Snort NGIPS powered by Talos Threat Intelligence. You'll have the latest threat telemetry powering automated response systems to keep your networks secure

[Data Center]
The Cisco Firepower 4000 series appliances are designed for high throughput computing environments and dedicated hardware for encrypted traffic inspection. By upgrading, you'll also gain high-availability and clustering, Cisco Threat Grid integration for sandboxing, and multi-instanced containerization of logical firewalls for maximum performance.

[Service Provider / Cloud]
The Cisco Firepower 9000 series hardware is designed for high-performance computing environments and provides low latency, high bandwidth, and NGIPS capabilities. Your networking environment will gain an 80% performance improvement and 33% improved encrypted traffic inspection speeds compared to previous generation Cisco SM models, ensuring your datacenter is scalable, highly available, and has optional DDoS protections needed for modern networking security.

[Existing Cisco ASA Customers]: If you are an ASA customer, you can gain fully integrated ACI security with a single point of control for network and security management. ASA customers can also leverage programmable automation for deployment and management, along with a common policy-based operational model.

Follow up with security challenges questions on the next page.

Could you tell me what kind of security challenges your organization faces?

(Call recipient describes the primary challenges their organization needs to overcome)
Understand their pain points and direct them towards potential Cisco solutions organized by the following general categories.

[Policy Management]: Cisco NGFW solutions helps prevent and eliminate policy sprawl through a centralized policy management portal that allows you to manage a consistent security policy across your entire organization's networking environment.

If call recipient expresses interest, follow up with Cisco Defense Orchestrator policy management features, and offer to send marketing materials or learning resources.

[Security Controls / Management]: Cisco technologies like Cisco Defense Orchestrator and Cisco Threat Response provide simplified management and exist as part of a global network of automated threat intelligence and defense and are deeply integrated across Cisco's NGFW portfolio.

If call recipient expresses interest, follow up with additional Cisco Defense Orchestrator / Cisco Threat Response features, and offer to send marketing materials or learning resources.

[Threat Efficacy]: Talos Threat Intelligence research underpins all of Cisco's security products, providing real-time actionable intelligence on the latest threats, and automation to ensure your infrastructure is proactively protected at every level.

If call recipient expresses interest, follow up with additional Cisco Threat Response / Snort NGIPS / Talos features, and offer to send marketing materials or learning resources.

[Intrusion Prevention and Malware Protection]: Both powered by Talos Threat Intelligence, Cisco's world-leading open-source Snort NGIPS is the golden standard for preventing malicious attacks against your network, and Cisco AMP for Network protects against the most sophisticated malware.

[Integration Gaps]: Cisco is the world-leader when it comes to enterprise networking, and our security offerings are tightly integrated into our proven solutions. We work with hundreds of security and networking vendors to ensure functional integration across a variety of point security products. Our integrations eliminate security gaps and protect against emerging multi-vector security threats.

If call recipient expresses interest, follow up with Cisco Threat Response features, and offer to send marketing materials or learning resources.

Refer to next page for instructions if call recipient indicates their organization faces no major challenges.

(Call recipient indicates that their organization faces no major challenges)

That's good to hear. Could you elaborate on what networking security infrastructure you have? I'd be disappointed if there was something I could do to help, but simply lacked the correct context. For example, here are some typical challenges we've seen countless organizations face:

Try to gauge which area is most applicable based on previous dialogue and pick one or two examples to provide context.

[Policy Management]: We've seen many occasions where outdated security policy management practices, inconsistent policies and human error leads to breaches and attacks. Does your organization struggle to manage security policies across your entire network environment?

(Call recipient responds positively) **Follow up with Consistent Policy and Visibility on next page.**

(Call recipient responds negatively) Are you sure your organization wouldn't benefit from a centralized security policy management solution? You could gain the ability to manage, monitor, and enforce all security policies from one dashboard.

[Evolving Threats]: Threats have become more sophisticated and networks have become more complex. Very few, if any, organizations have the dedicated resources to stay up to date and successfully fend off the latest emerging and evolving threats.

(Call recipient responds positively) **Follow up with World Class Security Controls on next page.**

(Call recipient responds negatively) Are you sure you wouldn't benefit from catching threats that are passing through your firewall that you may not know? We'd love to show you a demo of threats that could be passing through your system that you may not know about.

[Encrypted Traffic Inspection]: As the amount of encrypted traffic continues to rise, attempting to decrypt and scan such large volumes of traffic becomes prohibitively taxing on your network performance. We believe customers need a better way to protect their data, applications, and networks while leveraging encryption without losing performance.

(Call recipient responds positively) **Follow up with Cisco NGFW hardware decryption specs.**

(Call recipient responds negatively) Your organization can gain a significant increase in encrypted traffic inspection performance across your network with compared to previous generation firewalls, especially with how many devices need to be simultaneously connected.

[Broad Scope Of Security Needs]: As organizations IT infrastructure continues to become more diverse, spanning the data center, branch offices, multiple clouds, and end-user devices, the job of securing everything becomes more dynamic. The firewall has evolved to become more flexible, more granular, and more responsive, requiring a broader set of capabilities with deeper integrations.

(Call recipient responds positively) **Follow up with Turn Your Existing Network into an Extension of Security Architecture below.**

(Call recipient responds negatively) Does your IT / Networking / Security team feel like they can adequately deal with the incoming threats that will occur in the future? You may be adequately protected today, but new threats are constantly evolving to be increasingly robust and multi-pronged, often exploiting multiple vulnerabilities across various disparate systems.

(Call recipient continues to be unconcerned about potential challenges)

That's impressive, it seems like your organization is really on top of its network security needs. Given the dangers of emerging security threats and the potentially millions of dollars at risk, do you have 15 minutes to explore some additional security options?

(Call recipient says NO) **Thank them for their time and consider following up via email with marketing assets.**

(Call recipient says YES) **Utilize following examples to provide greater context for Cisco NGFW capabilities**

[Consistent Policy And Visibility]: By buying an updated NGFW appliance today, you will not only be gaining a stronger security posture today, but you will set yourself up with a future-ready management experience that can evolve alongside your network.

[Unified Management]: In the coming months, Cisco will be releasing integrations with Cisco Defense Orchestrator that enable streamlining of security policy and device management across your extended network, allowing you to accelerate key security operations such as detection, investigation, and remediation.

[World Class Security Controls]: Protect your networks against an increasingly complex set of threats with a complete portfolio of enforcement points deployed wherever you need them – including next-generation firewalls, intrusion prevention, secure internet gateways, malware protection, threat intelligence, and more. Your existing networking infrastructure can be supercharged with NGFW and NGIPS capabilities. You can also leverage dedicated hardware for encrypted traffic inspection without driving down performance.

[Turn Your Existing Network Into An Extension Of Security Architecture]: Trust your network security with the world leader in enterprise networking, giving you the deepest integrations between core networking functions and critical networking security capabilities. The result is a complete security portfolio that protects everything, everywhere. With Cisco you can easily extend security capabilities to switches and routers.

Additional Questions:

Utilize these questions if the customer is not providing enough context

1. How many point security products have you needed to install, manage, and update to remain proactive when it comes to defending your business against the latest emerging threats?
   Depending on answer, talk about the unified management, consistent policy and visibility responses on previous page.

2. Are you having challenges remediating policy sprawl across your networking security infrastructure?
   Depending on answer, talk about policy management on page 3

3. How comfortable are you that your existing security infrastructure could automate threat remediation against the latest evolving threats?
   Depending on answer, talk about encrypted traffic Inspection, evolving threats or broad scope of security needs from page 3

Call To Action:

Thank you for your time. Before we determine next steps and schedule a potential follow up call, I'd like to send you additional resources to highlight Cisco's NGFW portfolio. Can you please verify your contact information? And are there specific networking security topics you'd like me to send you additional resources on?

Resources to send depending on customer:

- 1000 Series Datasheet
- 2100 Series Datasheet
- 4000 Series Datasheet
- 9000 Series Datasheet
- NGFW-at-a-Glance
- NGFW Solution Overview