SOPHOS

Appliance Support Guide

INTRODUCTION

This document provides answers to common questions regarding the Sophos Appliance for Sophos NDR and Appliance Integration deployments. This guidance will help you understand the solution and what factors to consider when scoping a deployment.

To ensure successful implementation, please verify the solution requirements are met and pre-deployment tasks have been completed prior to deployment.

TECHNOLOGIES & CONCEPTS

In this section, we'll explain the different technologies used by the Sophos Appliance and how they could be applicable to your implementation.

Network Detection & Response

An organization's attack surface is ever evolving. Securing both known and unknown assets is an enormous task. Skilled attackers will use these vulnerable devices to carry out their attacks, while evading detection and covering their tracks. To stop these advanced threats, it's critical to have comprehensive network visibility to observe the attacker's lateral movement between segments.

Network Detection and Response (NDR) solutions continuously monitor network traffic for both known and unknown threats using a combination of signature-based controls and advanced methods, which include machine learning and behavioral analytics.

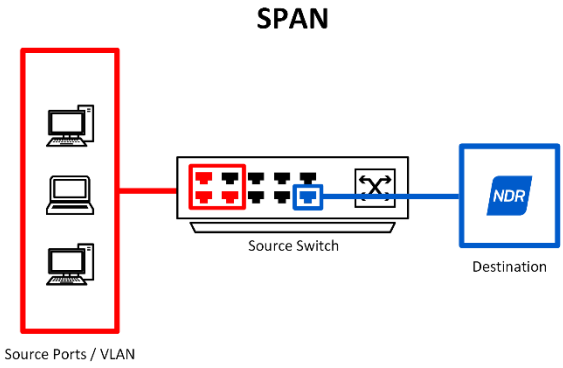
Sophos NDR acquires network traffic using port mirroring as described below.

SPAN

Often referred to as port mirroring—**Switched Port Analyzer (SPAN)** is a feature supported by most network switches that mirrors traffic from one or more interfaces or VLANs to a destination interface on the same switch. This is most often used for network traffic analysis tools to detect malicious activity.

Each switching platform support different options for the selection of traffic being mirrored, here are some examples:

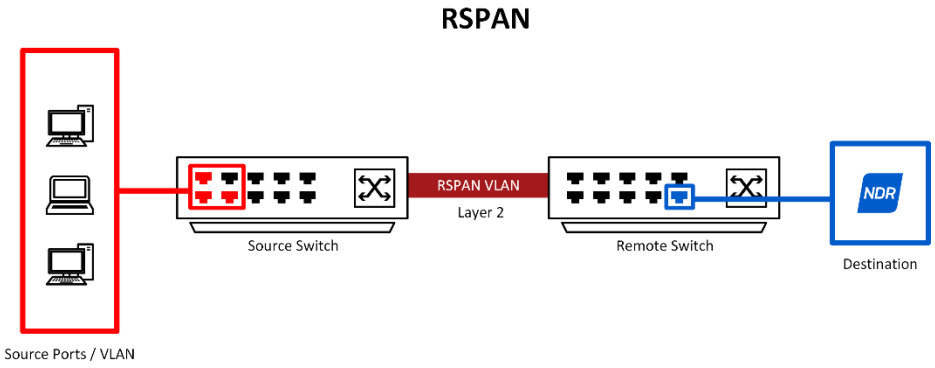
- **Physical Port(s)** – Copies all traffic sent/received by the source port(s) to the destination port
- **Trunk Port** – Copies all traffic for tagged VLANs on the source trunk port to the destination port
- **VLAN** – Copies all traffic traversing a VLAN to the destination port
- **Ingress SPAN** – Copies traffic received by the source ports/VLANs to the destination port
- **Egress SPAN** – Copies traffic sent by the source ports/VLANs to the destination port



RSPAN

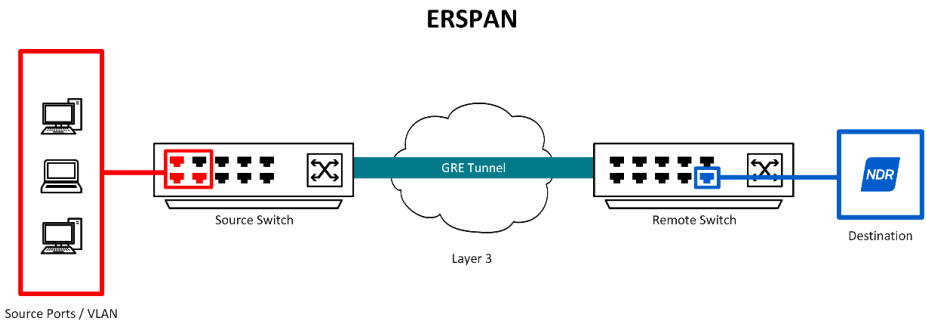
Remote SPAN (RSPAN) is an extension of SPAN that uses a special VLAN to mirror traffic from source ports and VLANs distributed over multiple switches, then sends that traffic to a centralized destination.

Each RSPAN session carries mirrored traffic over a dedicated VLAN in all participating switches. This VLAN is then trunked to other switches, allowing the RSPAN VLAN to traverse multiple switches.



ERSPAN

Encapsulated Remote SPAN (ERSPAN) as the name indicates—encapsulates SPAN traffic using generic routing encapsulation (GRE), making all captured traffic routable across a Layer-3 network. This is ideal for organizations that are unable to transport Layer-2 SPAN/RSPAN traffic to the desired network capture device.



SYSLOG

System Logging Protocol (SYSLOG) is a standard protocol used to send system log or event messages to a server. Using this protocol, logs can be collected from servers, firewalls, network switches and other devices in a central location for monitoring and review.

When licensing either the Firewall Integration or Network Integration Packs—the Sophos Appliance events using SYSLOG.

SOPHOS APPLIANCE OVERVIEW

The Sophos Appliance is designed to run one or more on-premise integrations which feed telemetry to the Sophos Data Lake. These integrations are deployed and managed via Sophos Central. The appliance is Ubuntu-based and uses K3s (a lightweight version of Kubernetes) for application orchestration and upgrades. The Sophos Appliance delivers the following solutions:

- **Sophos NDR** – Analyzes network flows for traffic patterns to identify advanced threats
- **Appliance Integrations** – Agent for collecting security events from 3rd party integrations

It's possible to deploy the appliance in any number of configurations—this includes multiple integrations with Sophos NDR. Currently, the Appliance supports deployment on the following platforms:

- VMware ESXi
- Microsoft Hyper-V
- Amazon AWS (Q3 2023)
- Microsoft Azure (Q3 2023)

A physical appliance is currently in development and planned for release in 2024.

SOLUTION REQUIREMENTS

Review the following items to ensure all of the solution requirements have been met.

CPU Requirements

To ensure compatibility with underlying technologies, the CPU of the system running the Sophos Virtual Appliance must support the following instruction sets:

Instruction Set	CPU Flag	Dependency
1 Gigabyte Pages	pdpe1gb	**Sophos NDR –** Packet processing workloads require large pages from memory to ingest network traffic
Advanced Vector Extensions 2	avx2	**Sophos NDR** - Leveraged by machine learning models for image recognition **Appliance Integrations** – Required by regex matching library used by Appliance Integration Agent agent

The CPUs referenced below support these instruction sets.

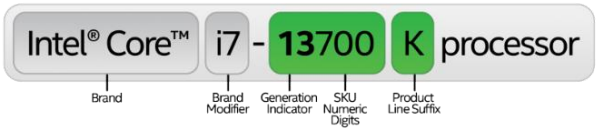
Supported Intel CPU Microarchitectures

Microarchitecture	Generation	Codename	Release Date
Skylake	6	Skylake	Q3 2015
	7	Kaby Lake	Q2 2017
	8	Coffee Lake	Q4 2018
	9	Cascade Lake	Q2 2019
	10	Comet Lake	Q2 2020
Palm Cove	10	Cannon Lake	Q2 2018
Sunny Cove	10	Ice Lake	Q3 2019
Cypress Cove	11	Rocket Lake	Q2 2021
Golden Cove	12	Alder Lake	Q1 2022

Raptor Cove	13	Raptor Lake	Q1 2023

For assistance with identifying Intel CPU microarchitecture generations, refer to the figure below:

Intel CPU Naming Convention



Generation Indicator must be 6 or higher

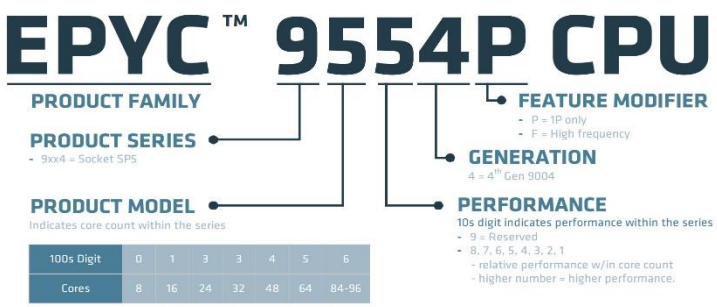
Supported AMD CPU Microarchitectures

Microarchitecture	Generation	Codename	Release Date
Zen	1	Naples	Q2 2017
		*Great Horned Owl	Q1 2018
Zen 2	2	Rome	Q3 2019
Zen 3	3	Milan	Q2 2021
Zen 4	4	Genoa	Q4 2022

*AMD Ryzen Embedded V1000 Series

For assistance with identifying AMD CPU microarchitecture generations, refer to the figure below:

AMD CPU Naming Convention



Compatible with every EPYC CPU generation

NOTE

For the most up-to-date CPU requirements, please refer to the following support article:

[Sophos Appliance - CPU Requirements]

Minimum System Requirements

The minimum system requirements are the same on all platforms.

On VMware, the OVA image is pre-configured to meet the minimum requirements for both Sophos NDR and Sophos Appliance Integration deployments. The requirements are as follows:

- 4 CPUs
- 16GB RAM
- 160GB storage

Depending on the workload of the Sophos Appliance, you may need to adjust the sizing of the virtual machine according to the **Sizing Recommendations**.

VMware Requirements

Here are the requirements for deploying the Appliance in VMware ESXi:

- VMware ESXi 6.7 or later
- VMware Enhanced vMotion Compatibility (EVC) Modes
  - EVC Level L8 – Intel "Skylake" Generation or higher
  - EVC Level B4 – AMD "Zen" Generation or higher
- VM hardware version 11 or higher

- Satisfy **CPU Requirements**
- If the workload of the appliance exceeds the parameters specified in **Sizing Recommendations**, adjust allocation of resources in alignment Sophos guidance

NOTE

To determine which version of VMware ESXi you have, refer to the following articles:

Determining the build number of VMware ESX/ESXi and VMware vCenter Server (1022196)

Build numbers and versions of VMware ESXi/ESX (2143832)

For the most up-to-date Sophos NDR VMware requirements, please refer to the following support article:

Sophos Appliance - VMware ESXi Requirements

Hyper-V Requirements

Here are the requirements for deploying the Appliance in Microsoft Hyper-V:

- Hyper-V version 6.0.6001.18016 (Windows Server 2016) or later
- Processor Compatibility Mode is **not supported**
- Comply with **Minimum System Requirements**
- Satisfy **CPU Requirements**
- If the workload of the appliance exceeds the parameters specified in **Sizing Recommendations**, adjust allocation of resources in alignment Sophos guidance

NOTE

To determine which version of Hyper-V you have, refer to the following article:

Identifying your Hyper-V Version

For the most up-to-date Sophos NDR Hyper-V requirements, please refer to the following support article:

Sophos Appliance - Microsoft Hyper-V Requirements

Mirroring Traffic from Physical Networks

When deploying Sophos NDR as a virtual appliance, extra steps must be taken to feed traffic from your physical network to the hypervisor. To facilitate bridging the physical and virtual networks, a mirror port must be configured to copy network traffic from source ports (or VLANs) to a destination port connected to the physical Ethernet interface of your virtual host.

NOTE

For more information on how to configure port mirroring on a Sophos switch, please refer to the online documentation:

Sophos NDR – Configure a Physical Switch

If you are using a different network vendor, make sure to follow the manufacturer's guidance for configuring SPAN. Please ensure to reference the most current documentation relevant to the switch model(s) and firmware version(s) in use.

NOTE

If a physical Ethernet adapter isn't available and the network switching solution in use supports ERSPAN—a virtual interface can be used by the NDR appliance to consume an ERSPAN feed.

For more information, please refer to the online **Sophos Appliance - Requirements**.

SOPHOS NDR

Overview

Sophos NDR continuously monitors network traffic to detect suspicious activities that may be indicative of attacker activity, leveraging a combination of machine learning, advanced analytics, and rule-based matching techniques.

It detects a wide range of security risks, including rogue devices (unauthorized, potentially malicious devices that are communicating across the network), unprotected devices, insider threats, zero-day attacks, and threats involving IoT and OT devices.

Sophos NDR monitors east/west (internal) traffic and north/south (outgoing/incoming) traffic to detect and flag anomalies indicative of threat activity. Sophos NDR detections include:

- Network scanning activity
- Unexpected SSH sessions to never-before accessed systems

- Suspected beaconing activity
- Suspected C2 connections
- Communication on non-standard ports
- Malware present in encrypted traffic
- Encoded PowerShell execution
- Abnormal volumes of data sent

Sizing Recommendations

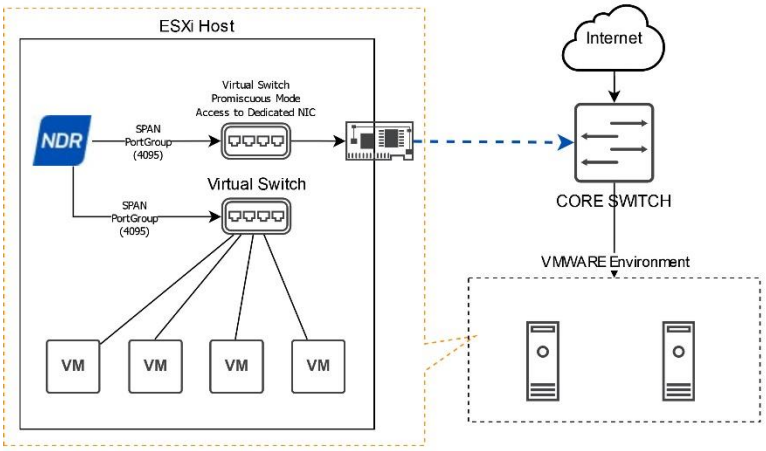
Each Sophos virtual appliance needs to be sized in accordance with the amount of network traffic being analyzed. These sizing recommendations are listed below:

Medium Traffic ▪ Up to 500 Mbps ▪ Up to 70,000 packets per second ▪ Up to 1,200 flows per second	Deploy virtual appliance using default hardware configuration ▪ 4 vCPUs ▪ 16 GB RAM ▪ 16 GB storage
Large Traffic ▪ Up to 1 Gbps ▪ Up to 300,000 packets per second ▪ Up to 4,500 flows per second	Increase the virtual appliance hardware configuration to use 4 additional vCPUs ▪ 8 vCPUs ▪ 16 GB RAM ▪ 16 GB storage

Deployment Scenario Examples

Scenario 1 – Core Layer

For organizations that aggregate network traffic from all segments to a backbone or core switch—Sophos NDR can easily ingest traffic from each desired VLAN or port by mirroring the trunk port(s) that connect to the firewall or gateway. With all connectivity between segments being routed through the core switch, Sophos NDR will have the flexibility to monitor traffic that's important to the organization.



VM and External Traffic Monitoring with Regular VMWare Port Mirroring

Advantages

Core Visibility – The core switch is the central point in the network through which all traffic passes through, which means that monitoring at this layer provides comprehensive coverage of all network traffic.

Reduced Complexity – Placing the NDR appliance at the core switch layer results in a high amount of network visibility with a relatively simple deployment. In most cases, the majority of traffic between networks is captured, in addition to North/South traffic.

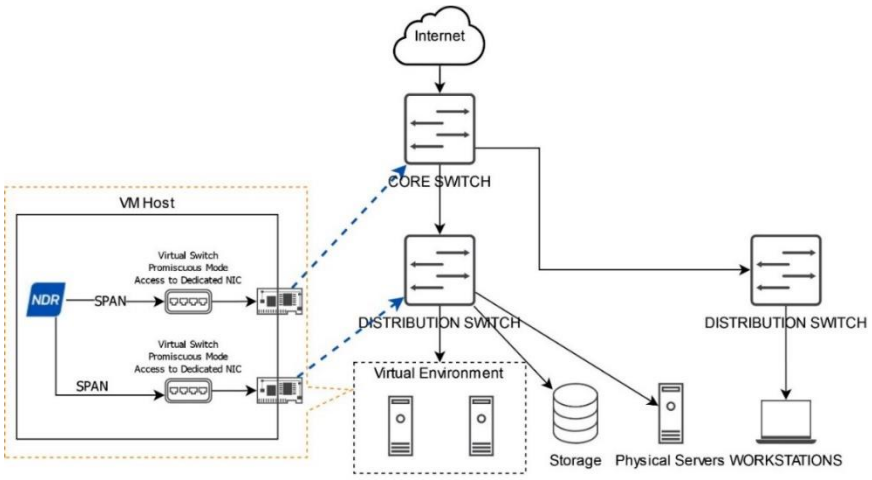
Disadvantages

Limited East/West Visibility – Placing the NDR appliance only at the Core layer may not provide sufficient visibility into traffic that only traverses the Distribution layer. This can limit the ability of the NDR appliance to detect attacks that take target these segments.

Lack of Redundancy – If the core switch fails or is compromised, the NDR appliance may be affected. This could lead to gaps in network visibility and security monitoring.

Scenario 2 – Core and Distribution Layer

In cases where core coverage isn't sufficient—the addition of ingesting network traffic from the distribution layer can provide enhanced East/West visibility between sites and/or network segments.



Advantages

Broader East/West Visibility – Deploying an NDR appliance at both the Core and Distribution layers adds more east/west visibility at a specific site. This enables network traffic from multiple switches to be monitored and analyzed for potential threats.

Traffic Source Redundancy – In the event of a switch failure, there are additional sources of network traffic for NDR to monitor, preventing a full gap in visibility.

Disadvantages

Prioritization of Visibility – Introducing the distribution layer for monitoring may introduce situations where additional overhead is required to run Sophos NDR. If there are limited resources available in the environment, you may need to evaluate which switches or network segments are most important to monitor.

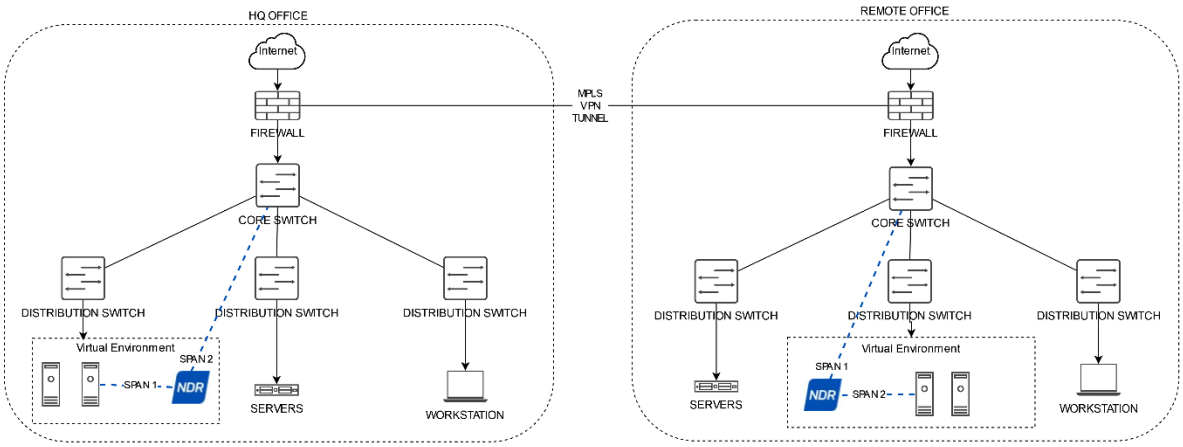
Limited to Vendor Support – This type of deployment may require RSPAN or ERSPAN, which is not available on all networking solutions. This lack of support could prevent specific sites or switches from being monitored by NDR.

Duplication of Telemetry – Additional planning will be necessary to prevent NDR from monitoring duplicated traffic. Mirroring redundant traffic is a waste of resources and could lead to duplication of detections.

Oversubscription – With more traffic being ingested, it's possible to oversubscribe the destination port connected to the capture interface on the NDR appliance. If this were to occur, the network switch would prioritize delivering actual network traffic over mirroring the traffic, resulting in a gap of network visibility.

Scenario 3 – Multi-site

For organizations with multiple sites it may be necessary to route SPAN traffic over WAN links or VPN tunnels in order to achieve better visibility. In this situation, SPAN traffic can be encapsulated in a GRE or VXLAN tunnel (otherwise known as Encapsulated Remote SPAN) to securely send the mirrored traffic from a remote site.



Advantages

Comprehensive Visibility – By utilizing ERSPAN and multiple NDR appliances, it's now feasible to monitor both local and remote locations for threats. If the switching environment at the remote site supports ERSPAN but lacks virtualization infrastructure, it wouldn't be necessary to deploy an NDR appliance at that location. Instead, you could encapsulate that traffic and send the feed to the NDR appliance at the HQ office.

Load Distribution – By distributing the load across multiple NDR appliances, there is more overall capacity available to distribute between appliances, enhancing coverage and resilience.

Traffic Source Redundancy – In the event of a switch failure, there are additional sources of network traffic for NDR to monitor, preventing a full gap in visibility.

Disadvantages

Bandwidth Limitations – While ERSPAN facilitates traffic mirroring from distant switches or locations where Sophos NDR cannot be deployed—ERSPAN can use a significant amount of resources and bandwidth sending that traffic. Ensure there is adequate bandwidth along the routed path that carries the mirrored traffic.

Limited to Vendor Support – This type of deployment will require ERSPAN, which is not available on all networking solutions. This lack of support could prevent specific sites or switches from being monitored by NDR.

Duplication of Telemetry – Additional planning will be necessary to prevent NDR from monitoring duplicated traffic. Mirroring redundant traffic is a waste of resources and could lead to duplication of detections.

Oversubscription – With more traffic being ingested, it's possible to oversubscribe the destination port connected to the capture interface on the NDR appliance. If this were to occur, the network switch would prioritize delivering actual network traffic over mirroring the traffic, resulting in a gap of network visibility.

Best Practices

Considerations for Deployment

When network traffic is being collected from numerous sources and aggregated together for analysis—it's relatively easy to oversubscribe a destination SPAN port or NDR appliance. Use a selective approach when deciding which traffic to mirror. Most often, it's undesirable to inspect all traffic within an environment, instead focus on traffic that is most important to your organization's security.

Prior to implementation, here are some other important factors to contemplate:

- Which locations are in scope for monitoring?
- Which network segments would an attacker likely target?
- How would you prioritize which network segments to monitor?
- Does each site have a networking stack capable of mirroring network traffic?
- Where should the Sophos NDR appliance be deployed to get visibility into the traffic of interest?
- Do any of the in-scope networks use NAT which could hide source IP/MAC addresses?
- Does my virtual environment meet the solution requirements?
- Which virtual hosts are suitable to host Sophos NDR? Any available physical network interfaces?

Data Acquisition Recommendations

At first, be conservative – When deciding which network traffic to bring into Sophos NDR—prioritize which traffic should be monitored initially, then gradually bring in the additional sources to ensure there are no issues.

Avoid redundancy of captured traffic – Be mindful not to include mirror sessions that are already being observed by other Sophos NDR appliances. If there are other pre-existing mirror sessions or sessions being consumed more than once, it is wasteful of resources and could lead to a lack of visibility. To prevent this issue, map out which ports or VLANs are being monitored by each SPAN session so network traffic isn't being duplicated.

Oversubscription can be an issue – When selecting a range of ports or VLANs to mirror, think about the available bandwidth available on the corresponding destination SPAN port. Network switches prioritize

actual network traffic. If the destination SPAN port is saturated, Sophos NDR will never receive the mirrored traffic.

Some types of traffic should not be mirrored – While it might be tempting to monitor all network traffic—there are certain types of networks that have limited usefulness to monitor or could cause disruptions if mirrored. Do not include ports or VLANs that are carrying the following types of traffic:

- **WAN traffic** – When mirroring traffic, be cognizant to exclude WAN interfaces from the SPAN session. There is little value in analyzing this traffic due to the volume of port scanning and other activities. If there is an external-facing application in a DMZ you want to monitor with Sophos NDR—ensure the interface being mirrored is internal to the perimeter.
- **Storage Area Network (SAN) traffic** – Analyzing storage area networks for malicious activity often proves to be more trouble than it's worth. The NDR appliance resources are better spent monitoring other networks and if your virtual environment is hosted on the SAN, could lead to disruption of services.
- **VMware Management Traffic** – Sophos recommends avoiding any mirroring of VMware management (VMkernal) traffic. This is likely to cause issues and doesn't provide a lot of benefit.
- **Voice over IP (VOIP) traffic** – It's not particularly advantageous to monitor VOIP traffic for anomalies. These networks are often saturated and eat up NDR resources. Instead, practice good network segmentation hygiene and observe VOIP gateways or other entry points to the broader network enviornment.

Options for traffic ingestion – In situations where the virtual host doesn't have a physical Ethernet adapter available, an ERSPAN virtual interface can be configured to collect the traffic.

Flexibility at a cost – While ERSPAN facilitates traffic mirroring from distant switches or locations where Sophos NDR cannot be deployed—ERSPAN can use a significant amount of resources and bandwidth sending that traffic. Ensure there is adequate bandwidth along the routed path that carries the mirrored traffic.

NAT obscures visibility – If Network Address Translation (NAT) is employed within your environment, it's possible that Sophos NDR will not be able to observe the true source IP address of the communication.

Design Considerations

Unlimited Appliances – There is no limitation to the number of Appliances that can be deployed. Use this to your advantage for optimal NDR sensor placement.

Sizing for two SPAN interfaces – Each NDR appliance supports two SPAN interfaces. If both interfaces are used, the appliance needs to be sized according to the **Large Traffic** configuration (8 vCPUs).

Consuming more than 1 Gbps – If there's a need to ingest more than 1 Gbps per appliance—deploy multiple NDR Appliances to divide traffic into smaller streams. If there is a requirement for bridging traffic from the physical network, additional dedicated Ethernet adapters will be required.

Directing traffic using VLANs – When deploying multiple NDR Appliances on the same virtual switch, SPAN traffic can be directed to the appropriate NDR appliance using VLAN tagging on the port group.

Running Multiple Integrations with Sophos NDR – The sizing recommendations apply to an appliance running only Sophos NDR. If the appliance is running one or more Appliance Integrations, additional resources may be required (see **Appliance Integration Constraints**).

Pre-Deployment Checklist

IMPORTANT

Due to the complex and often difficult nature of Sophos Appliance deployments, Sophos strongly recommends that customers purchase **Sophos Professional Services** to assist with the process.

It is also important to consider the appropriate personnel are involved with the scoping and deployment process. In many situations, the virtualization and networking environments are managed by different teams.

Minimum Requirements

Review the **Solution Requirements** section of this document to confirm that your infrastructure meets the deployment meets the criteria. If this infrastructure doesn't satisfy the minimum requirements, consider purchasing hardware and/or software that is suitable for the implementation.

Deployment Planning

To ensure a successful deployment, please gather and organize the following materials:

Virtual Environment	
Architecture	Virtual architecture diagrams or other documentation.
Host(s)	Number of hosts, including site affiliation.
Hypervisor	Virtualization platform and version(s).
CPU	Brand and model of CPU. Number of CPUs present.
RAM	Amount of installed memory. Current usage.

Network	Hardware Ethernet adapter speed(s). Number of adapters present and available.
Storage	Type of storage. Disk capacity with available space.

Network Architecture	
Required Material	**Recommended Material**
IP subnet information	Network topology diagrams
Site information	Inventory of firewalls, by vendor/model
VLAN information	Inventory of switches, by vendor/model
Internet connectivity bandwidth	Firewall firmware version(s)
Inter-site connectivity bandwidth	

Management Network – The customer will need to determine the appropriate network for the Sophos Appliance to use for connectivity to Sophos Central and whether to use DHCP or a static IP address.

Internet Connectivity – In order to properly communicate with Sophos Central—the Sophos Appliance requires the ability to perform certain actions or communicate using various protocols.

- Perform DNS lookups for name resolution
- NTP time synchronization
- Send and receive HTTP/HTTPS
- Send and receive DHCP traffic on configured management network

NOTE

For an exhaustive list of port and domain exclusions, please refer to the following support article:

Sophos Appliance - Port and Domain Exclusions

External-Facing Applications – If Sophos NDR will be monitoring an external-facing application, collect details about OS and application platforms and version. Information about how the application is protected from internet traffic (e.g. IP information, firewall configuration, port forwarding, etc.) will also be needed.

APPLIANCE INTEGRATIONS

Overview

Once a Sophos Firewall or Network Integration Pack is licensed and configured—an agent is deployed to the Sophos Appliance. The purpose of this application is to ingest security events from on-premise security devices, filter unwanted messages, then send this telemetry to the Sophos Data Lake. From there, the Sophos MDR Detection Pipeline normalizes, enriches, correlates and prioritizes security events. This data combined with insights from the endpoint and other tools accelerates a Sophos MDR analysts' incident response capability.

Sizing Recommendations

In most scenarios, deploying the Appliance with the default hardware configuration is sufficient. Based on the volume of events being collected, here are the Sophos recommendations for sizing a virtual machine for a Appliance Integration deployment.

MDR Integrations	Deploy VM using default hardware configuration. No changes required.
▪ Firewall Integration Pack ▪ Network Integration Pack	▪ 4 vCPUs ▪ 16 GB of RAM ▪ 160 GB storage

Best Practices

Appliance Integration Constraints

Each Sophos Appliance can support a maximum of 8,000 EPS (Events per Second). This limit applies regardless of the number of integrations added to the appliance. For rough context—this is equivalent to 691,200,000 events per day and approximately 1 Gbps of network traffic.

By default, the Appliance Integration Agent is allocated a maximum of 2 GB RAM. This should accommodate for up to 4 integrations per appliance. If more RAM is needed, this setting can be

increased via the Console UI. Expect the Appliance Integration Agent to use approximately 400 MB of RAM under heavy load.

Deployment Considerations

When sizing a Sophos Appliance an Appliance Integration Agent deployment, first determine:

- The number of integrations to be deployed
- Estimated average EPS (Events per Second) being ingested

After establishing these factors, design the deployment according to the guidance provided in this document. If it is projected that the SYSLOG of the source device(s) will exceed the 8,000 EPS limit, do one of the following:

- Reduce log types sent to Appliance Integration Agent
- Lower log verbosity level
- Use dedicated Sophos Appliance for the high volume log source, while deploying additional appliances for any other log source

Pre-Deployment Checklist

Minimum Requirements

Review the **Solution Requirements** section to confirm that the infrastructure being used for the Sophos Appliance deployment meets the criteria. If the planned infrastructure doesn't satisfy the minimum requirements—consider purchasing hardware and/or software that is suitable for the implementation.

IMPORTANT

Due to the complex and often difficult nature of Sophos Appliance deployments, Sophos strongly recommends that customers purchase Sophos Professional Services to assist with the process.

It is also important to consider the appropriate personnel are involved with the scoping and deployment process. In many situations, the virtualization and networking environments are managed by different teams.

Deployment Planning

Prepare the following material in advance deployment:

Management Network – The customer will need to determine the appropriate network for the Sophos Appliance to use for connectivity to Sophos Central and whether to use DHCP or a static IP address.

Appliance Connectivity – In order to properly communicate with Sophos Central—the Sophos Appliance requires the ability to perform certain actions or communicate using various protocols:

- Perform DNS lookups for name resolution
- NTP time synchronization
- Send and receive HTTP/HTTPS
- Send and receive DHCP traffic on configured management network

Syslog Interface – When deploying the Firewall or Network Integration Pack, the Sophos Appliance requires a static IP address to be assigned to a network interface dedicated to ingesting log events. This static IP address will be used for all integrations. For each integration deployed, a new port will be dynamically assigned by Sophos Central at the time of deployment. Ensure this interface is connected to the same network as the management interface of the firewall or network device Sophos is ingesting logs for.

Syslog Forwarding – Refer to the **Sophos Central Admin - Integrations** documentation for guidance on how to configure Syslog forwarding on your firewall or network device.

APPLIANCE SETUP

Sophos NDR

For the latest information about deploying a Sophos NDR appliance, please refer to the documentation located here:

Sophos NDR Documentation

Sophos Appliance Integrations

For the latest information about deploying a Sophos Appliance Integrations in VMware, please refer to the documentation located here:

Deploy a VM for Integrations - VMware

For the latest information about deploying a Sophos Appliance Integrations in, please refer to the documentation located here:

Deploy a VM for Integrations – Hyper-V

SUPPORT RESOURCES

Sophos Appliance

Sophos Appliance - Requirements – An up-to-date support article detailing the solution and provides guidance for configuration and deployment scenarios.

[Sophos Appliance - User Guide] – A guide to help you get started with the Sophos Appliance.

Sophos NDR

[Sophos NDR Documentation] – Support article providing technical requirements and implementation guidance for Sophos NDR.

[Sophos NDR VM Sizing Guide] – Recommendations for sizing the Sophos Appliance according to workload.

[VMware ESXi Deployment Video] – Video walkthrough of deploying Sophos NDR in VMware ESXi.

[Microsoft Hyper-V Deployment Video] – Video walkthrough of deploying Sophos NDR in Hyper-V.

[Sophos NDR Community Channel] – Find helpful resources and connect with other Sophos users.

[Analyzing Flow Based Detections] – In this video, NDR Product Manager Karl Ackerman explains how to interpret NDR flow-based detections.

Appliance Integrations

[MDR Integrations Documentation] – Review the most current information regarding supported integrations and how to deploy them.

[Troubleshooting MDR Integrations] – This article lists common issues when deploying third party integrations with Sophos Central.

TROUBLESHOOTING

If you encounter problems using the **Sophos Appliance**, this section will provide information to assist with the resolution of common issues.

Connectivity Issues with Sophos Central

Port & Domain Exclusions

If the Sophos Appliance is unable to connect to Sophos Central, it's possible there could be a firewall rule preventing it. If that's the case, please review the full list of port and domain exclusions and update your access policies to allow for Sophos Central connectivity:

[Sophos Data Collector Requirements - Port and domain exclusions]

Registration attempted with used/invalid OTP

If the Sophos Appliance displays a 'Registration attempted with used/invalid OTP' error, the one-time password for registering with Sophos Central has become invalid.

To resolve this issue, a new virtual appliance will need to be deployed. To resolve this issue, perform the following steps:

1. Sign in to Sophos Central
2. Go to Threat Analysis Center > Integrations > Data collectors
3. Document the configuration of the appliance
4. Delete the appliance
5. **Create a new appliance** according to the documented configuration
6. **Download the VM image**
7. **Redeploy the Sophos Appliance VM**

Problems with the Sophos Appliance Booting

If for whatever reason the Sophos Appliance will not book, ensure the virtual host meets the **CPU Requirements**. If the host is equipped with a supported CPU, check the following:

VMware ESXi

Verify that the VMware infrastructure meets the following criteria:

- The vSphere cluster's Enhanced vMotion Compatibility (EVC) mode baseline for applicable CPU microarchitecture is:
  - EVC Level L8 – Intel "Skylake" Generation or higher
  - EVC Level B4 – AMD "Zen" Generation or higher
- The Sophos Appliance VM hardware version is 11 or higher
- The Sophos Appliance virtual machine must have the following CPU flags enabled:

Instruction Set	CPU Flag
1 Gigabyte Pages	pdpe1gb

NOTE

For more information about VMware EVC Modes, please refer the following VMware articles:

Enhanced vMotion Compatibility (EVC) Explained

"The target host does not support the virtual machine's current hardware requirements" error vMotioning a VM (1003212)

Advanced Vector Extensions 2	avx2

Microsoft Hyper-V

Verify that the Hyper-V appliance does NOT have Processor Compatibility Mode enabled.

When using Processor Compatibility Mode, it ensures that the set of processor features available to virtual machines across a disparate set of virtualization hosts will match by presenting only a limited set of processor features to the virtual machine. However, hiding these features means that the guest operating system and application software cannot take advantage of these processor instruction set enhancements. As a result, intensive floating-point calculations required by the Sophos Appliance will not function.

Disable processor compatibility mode using PowerShell

To disable processor compatibility mode for a VM using PowerShell, shut down the VM and run the `Set-VMProcessor` cmdlet, setting `CompatibilityForMigrationEnabled` to `$false`, then restart the VM.

```
get-vm -name <name of VM> -ComputerName <target cluster or host> |
Set-VMProcessor -CompatibilityForMigrationEnabled $false
```

Hyper-V – Error when Deploying using PowerShell Script

If you encounter a *"Cannot be loaded because running scripts is disabled on this system"* error when deploying a Sophos Appliance in Hyper-V, this is due to insufficient permissions to execute PowerShell scripts.

NOTE

For more information about Hyper-V Processor Compatibility Mode, please refer the following Microsoft article:

[Processor Compatibility Mode in Hyper-V]

To change the PowerShell execution policy, perform the following steps:

Set Execution Policy to Bypass for Current PowerShell Process

1. Open PowerShell as Administrator
2. Enter the command below, then press enter:

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -f
```

After execution, the PowerShell execution policy will allow the current PowerShell process to run any PowerShell script without restrictions or security warnings. This will allow for the execution of the Sophos Appliance deployment script.

OPTIONAL

Once the Sophos Appliance has been successfully deployed, we recommend closing the PowerShell window and opening a new instance PowerShell to verify the Execution Policy is no longer set to 'Bypass' using the **`Get-ExecutionPolicy`** command.

Hyper-V – Capture Interface is Not Receiving Unicast Traffic

If the capture interface on the Sophos NDR appliance is not receiving unicast traffic, that typically indicates an unhealthy SPAN configuration. After confirming the configuration of SPAN is correct on your switch, it's possible that there could be an issue with the virtual networking configuration.

For Microsoft Hyper-V deployments, here are some additional steps to take if you encounter this issue. Sophos recommends shutting down the NDR virtual appliance prior to making any changes to the Hyper-V configuration.

- Ensure that the physical Ethernet adapter dedicated to collecting traffic on the Hyper-V host is connected to the correct SPAN destination port on the switch.
- Go to the Windows network configuration for the capture interface and unbind all services and protocols.
- In Hyper-V Manager, ensure the Sophos NDR capture interface is connected to the virtual switch attached to the physical Ethernet adapter.

- In Hyper-V Manager, go to the ‘Settings’ of the Sophos NDR VM. Next, under the properties of the capture interface, go to ‘Advanced Features’ -> ‘Port Mirroring’ and set the ‘Mirroring Mode’ to *Destination*.

NOTE

If any Sophos NDR capture interface is assigned an IP address, port mirroring will not work properly. It’s common Windows to self-configure a 169.254.x.x address using the Automatic Private IP Addressing (APIPA) feature.

To remedy this, please disable all services and protocols in the Windows network configuration of any in use capture interface.