Forcepoint

Web Security On-prem

v8.5.x

Network Agent Quick Start

Revision A

Contents

Introduction

Network Agent monitors Internet traffic for all or specified segments of a network. Its purpose depends on your subscription level and deployment:

- In both Forcepoint Web Security deployments and integrated Forcepoint URL Filtering deployments, Network Agent is an optional component that may be used to:
  - Manage non-HTTP requests
  - Provide enhanced logging
  - Manage Internet access based on bandwidth
  - Log bandwidth usage data

  With Forcepoint Web Security, Content Gateway can instead be used to manage protocols that tunnel over HTTP, and to provide some bandwidth management.
- In standalone Forcepoint URL Filtering deployments, Network Agent is a required component that manages both HTTP and non-HTTP traffic, enabling:
  - Policy enforcement
  - Network protocol and Internet application management
  - Bandwidth management
  - Logging of bytes transferred

When Network Agent is used to manage non-HTTP protocols, it can detect malicious peer-to-peer applications and spyware, even when they tunnel over ports commonly used for legitimate Internet communication. In addition, Network Agent can manage requests for Internet applications used for instant messaging, streaming media, file sharing, proxy avoidance, Internet mail, and other network or database operations.

This Quick Start introduces Network Agent and summarizes the steps needed to successfully deploy the component in your network.

Related concepts

Network Agent planning worksheets on page 5

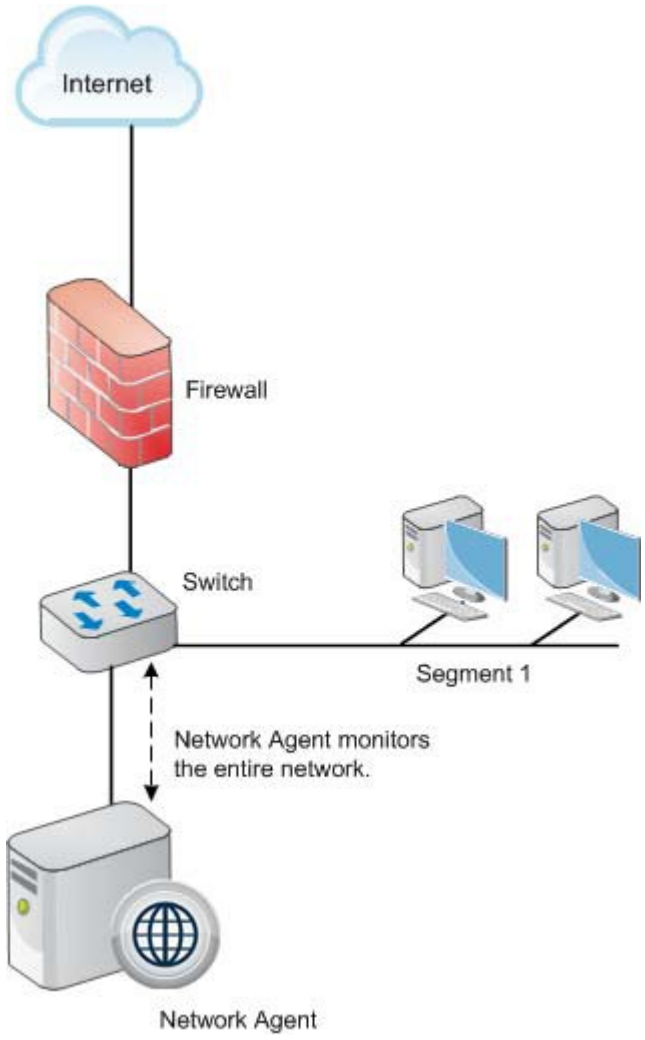
Configuring Network Agent on page 5

Related information
Deploying Network Agent on page 3
Troubleshooting tips for Network Agent on page 9

Deploying Network Agent

Where does Network Agent belong in the network?

Install Network Agent where it can see all Internet requests (HTTP and non-HTTP) from the machines it is assigned to monitor. This monitoring must be done inside the firewall.



Optionally, deploy multiple Network Agent instances, with each instance monitoring a different segment of the network. This may be necessary in a busy network.

The size and configuration of the network, the hardware capabilities of each Network Agent machine, and the volume and type of network traffic all play a role in determining how many Network Agent instances are needed. Some sites can use one Network Agent machine for every thousand users; others use one Network Agent machine for several thousand users. Forcepoint Technical Support and Sales Engineering can assist with deployment decisions.

Network Agent machines can connect to the network via a switch or hub.

Although Network Agent can be installed on the same machine as some integration products, it should never be installed on the same machine as the firewall.

If your network includes a router or Network Address Translation (NAT) device, position Network Agent to see the original (not the translated) IP addresses for all monitored machines.

Network interface cards (NICs)

Network Agent requires at least one network card (NIC) to monitor and block traffic, and can be configured to use multiple NICs. Each NIC that Network Agent uses for monitoring must be able to see all inbound and outbound traffic for the network or segment that it is configured to monitor.

Install and configure each NIC before installing Network Agent:

- Each NIC must be connected to a switch or hub and enabled in the operating system.
- The NIC used to monitor traffic must be configured to capture all packets on the network, not only the packets addressed directly to it (promiscuous mode).

If Network Agent is installed on a Linux machine make sure that either:

- The blocking NIC and monitoring NIC have IP addresses in different network segments (subnets).
- You delete the routing table entry for the monitoring NIC.

If both the blocking and monitoring NIC on a Linux machine are assigned to the same subnet, the Linux operating system may attempt to send the block via the monitoring NIC. If this happens, the requested page or protocol is not blocked, and the user is able to access the site.

If your network uses 802.1Q VLAN tagging, the NIC used to **monitor** Internet traffic connects to the switch port with a 802.1Q protocol header. The NIC used for **blocking** does not need to include the 802.1Q protocol header. As a result, it cannot be connected directly to trunk ports.

If you add a NIC after installing Network Agent, restart the Network Agent service, and then use the Web module of the Forcepoint Security Manager to configure the new NIC.

Connecting to a switch

If the Network Agent machine connects to a switch, the switch must support port spanning (mirroring). This means that a copy of all network traffic seen on the switch is sent to the span or mirror port for monitoring.

If you use a switch that supports bidirectional spanning (allowing packets to be monitored and sent from the same port), Network Agent needs only one NIC.

If your switch does not allow bidirectional traffic in spanning (mirroring) mode:

1) Use the NIC connected to the span port to monitor traffic.

2) Install a second NIC on the Network Agent machine. The NIC must have an IP address.

3) Attach the second NIC to a port that can communicate with all monitored machines and the Filtering Service machine.

4) Configure the second NIC as the blocking NIC.

Connecting to a gateway

In small to medium-sized Microsoft Windows environments, Network Agent can be installed on the gateway machine. This allows Network Agent to manage and monitor all Internet traffic. The gateway can either be a proxy server or a network appliance. Do not install Network Agent on a firewall.

In larger networks, performance can suffer as a result of resource competition between the gateway software and Network Agent.

Network Agent planning worksheets

Attached to this file are 4 PDF worksheets that you can use to capture all of the information you need to configure Network Agent for your environment.

- Worksheet 1: Identify your internal network (intranet) to ensure that Network Agent can separate internal network communication from Internet traffic.
- Worksheet 2: Associate each Network Agent machine with a Filtering Service instance.
- Worksheet 3: Identify proxy and cache machines and Network Agent ports.
- Worksheet 4: Assign a network card (NIC) to each segment of the network, with no overlap. Identify IP addresses that should not be monitored.

Configuring Network Agent

Use the Forcepoint Security Manager to configure Network Agent to recognize machines in your internal network, communicate with Filtering Service, monitor traffic from specified machines, log appropriate data, and more.

Configure Global settings

Before you begin

Refer to Planning Worksheet 1 for help in configuring Network Agent Global settings. All Network Agent instances in your network use these settings.

Steps

1) In the Web module of the Forcepoint Security Manager, go to the **Settings** > **Network Agent** > **Global** page.

2) Make sure that the **Ignore Internal Traffic** list includes all IP addresses in your network.

> **Important**
>
> This information is **not** used to determine which machines are monitored for policy enforcement. Instead, it allows Network Agent to ignore internal communications while monitoring Internet traffic.

An initial set of entries is provided by default. You can add additional entries, or edit or delete existing entries.

IP addresses and ranges in the list may use IPv4 or IPv6 format.

Be sure to include all IP addresses that are part of your network, whether or not you want Network Agent to monitor traffic to or from the machine. Later, you will configure whether Network Agent monitors traffic to specific internal IP addresses, and specify which IP addresses are monitored for outgoing Internet traffic.

- Click **Add** to add an IP address or IP address range to the list.
- Click an entry in the list to edit it.
- Mark the check box next to an entry, and then click **Delete** to remove it from the list.

IP address ranges in the list cannot overlap, and you cannot enter an individual IP address that falls within a range already in the list.

3) Use the **Internal Traffic to Monitor** list to specify internal IP addresses (included in the network definition list) for which you do want Network Agent to monitor connections from other internal IP addresses. You might include internal web servers, for example, to help track access to internal resources.

- Any requests sent from within the network to the specified internal machines is monitored by Network Agent. This traffic can be filtered and will appear in reports.
- By default, the list is blank.

4) Use the **Additional Settings** options allow you to determine how often Network Agent calculates bandwidth usage, and whether and how often protocol traffic is logged:

Field	What to do
Bandwidth calculation interval	Enter a number between 1 and 300 to specify how frequently, in seconds, Network Agent should calculate bandwidth usage. An entry of 300, for example, indicates that Network Agent will calculate bandwidth every 5 minutes. The default is 10 seconds.
Log protocol traffic periodically	Mark this option to log protocol traffic for use in reports, and to enable the Logging interval field.
Logging interval	Enter a number between 1 and 300 to specify how frequently, in minutes, Network Agent logs information about protocol traffic. An entry of 60, for example, indicates that Network Agent will write to the log file every hour. The default is 1 minute.

5) When you are finished making changes, click **OK** to cache the changes. Changes are not implemented until you click **Save and Deploy**.

Configure local settings

Before you begin

Refer to Planning Worksheets 2 and 3 for help in configuring local settings. Only the selected Network Agent instance uses these settings.

Steps

1) Under **Settings** > **Network Agent**, highlight or mouse over **Global**, then select the IP address of the Network Agent instance that you want to configure.

   When the local settings page opens, the IP address of the selected instance appears in the title bar at the top of the content pane.

2) Select the **Filtering Service IPv4 address** that identifies the Filtering Service instance with which this Network Agent will communicate (Planning Worksheet 2). If Network Agent and Filtering Service are installed on the same machine, the local IP address is selected by default.

3) Indicate whether Network Agent should block or permit all requests **If Filtering Service is not available**.

4) Under the **Network Interface Cards** list, use the **Proxies and Caches** list to specify any proxy or cache machines that monitored machines use to access the Internet. This keeps Network Agent from identifying requests from both the client machine and the proxy or cache machine, which could result in duplicate log records or incorrect filtering.

   Click **Add** to include a proxy or cache IP address in the list.

5) Expand **Advanced Network Agent Settings**.

   a) With Forcepoint Web Security, or when Forcepoint URL Filtering is integrated with a third-party product, verify that the **Integration manages HTTP traffic on ports** value is correct. (The default is 80, 8080.)

      If you have installed your web protection software in standalone mode, all ports are monitored and the field is disabled.

   b) If you want Network Agent to ignore traffic on specific ports, mark **Configure this Network Agent instance to ignore traffic on the following ports**, and then enter one or more ports in a comma-separated list.

      This may be used to prevent double logging of HTTPS traffic.

   Do not make changes to the **Debug Settings** options unless directed to do so by Technical Support.

6) Click **OK** to cache your changes. Changes are not saved until you click **Save and Deploy**.

Configure NIC settings

Before you begin

Refer to Planning Worksheet 4 for help in configuring NIC settings. These settings determine which NIC is used for monitoring and which is used for blocking and communication with other web protection components. They also determine which IP addresses this Network Agent instance monitors, and how the agent responds to requests for non-HTTP protocols.

Steps

1) Click an entry in the **Network Interface Cards** list on the Local Settings page for the Network Agent instance that you are configuring.

   The **NIC Information** list provides a description of the selected network card.

2) Indicate whether or not to **Use this NIC to monitor traffic**.

   If the Network Agent machine has multiple NICs, you can configure more than one NIC to monitor traffic.

   - If this NIC will be used for monitoring, click **Configure**, and continue with step 3.
   - If this NIC will not be used for monitoring, go to step 4.

3) Use the **Local Settings** > **NIC Configuration** > **Monitor List** page to configure monitoring behavior:

   - Use the **Monitor List** to identify which IP addresses (All, None, or Specific) this Network Agent instance monitors.

     If you select Specific, add the IPv4 or IPv6 address ranges and individual IPv4 or IPv6 addresses that this Network Agent should monitor.
   - Under **Monitor List Exceptions**, add any IP addresses within the monitored ranges that Network Agent should not monitor.
   - When you are finished making changes, click **OK** to return to the NIC Configuration page.

4) Indicate which NIC Network Agent should use as a **Blocking NIC**. This NIC is also used for communication with other web protection components, and must have an IP address.

5) If you have Forcepoint Web Security, or if Forcepoint URL Filtering is integrated with a third-party product:

   - Select **Log HTTP requests** to improve reporting accuracy.
   - Select **Filter all requests not sent over HTTP ports** to use Network Agent to manage only those HTTP requests not sent through the integration product.

     If you are running Forcepoint URL Filtering in Stand-Alone mode, Filter and log HTTP requests is selected, and cannot be changed.

6) Under **Protocol Management**, indicate whether Network Agent should be used to Filter non-HTTP protocol requests and Measure bandwidth by protocol.

   Click **OK** to cache your changes, and then click **Save and Deploy** to implement them.

Next steps

After configuring Network Agent, you may want to use a packet analyzer to ensure that the monitoring NIC is able to see traffic from all of the IP addresses that it is configured to monitor.

Wireshark is a free, popular, open source network protocol analyzer, available for Windows and Linux systems from www.wireshark.org.

If traffic from some IP addresses is not visible:

- Review the network configuration and NIC placement requirements.
- Review Deployment and Installation Center for more detailed network configuration information.
- Verify that you have properly configured the monitoring NIC.

Troubleshooting tips for Network Agent

Network Agent cannot contact Filtering Service

When Filtering Service has been uninstalled and reinstalled, the Network Agent does not automatically update the internal identifier (UID) for Filtering Service.

To re-establish connection to Filtering Service:

Steps

1) Open the Web module of the Forcepoint Security Manager and select **Settings** in the left navigation pane.

2) Expand the **Network Agent** section, and then select a Network Agent IP address.

3) Select the **Filtering Service IPv4 address** from the drop-down list.

4) Click **OK** to cache your changes, and then click **Save and Deploy**.

Network Agent fails to start with stealth mode NIC

On Linux systems that include a network card configured in stealth mode, there are 2 potential issues that may prevent Network Agent from starting:

- A stealth mode NIC may inadvertently be selected for communication (blocking) during installation. Use the Security Manager to select a different blocking NIC.
- If Network Agent is bound to a NIC configured for stealth mode, and then the NIC IP address is removed from the Linux configuration file (`/etc/sysconfig/ network-scripts/ifcfg-`<*adapter name*>), Network Agent will not start.

To reconnect Network Agent to the NIC, restore the IP address in the configuration file.

Spanning or mirroring is configured incorrectly

If Network Agent is connected to a switch, it must be able to see all traffic for the network or segment that it monitors. This means that it must connect to the span, mirror, or monitor port (though the term varies by manufacturer, the function is the same).

The span port mirrors all the traffic that leaves the network segment, so traffic is simultaneously sent to the monitoring port to which Network Agent is connected.

Monitor (span, mirror) only the port going to the firewall or router, not the entire network.

Router or firewall traffic is being monitored in the wrong direction

Monitor (span, mirror) the traffic going to the firewall or router. On Cisco switches, this means you need to specify **Tx**. On HP and 3Com switches, you need to specify **Egress**.

To log bytes sent and received, set both **Tx** and **Rx** (Cisco) or both **Egress** and **Ingress** (HP, 3Com).

Teamed NICs

Teamed NICs share the load under one common identity, with multiple adapters load- balancing under a single IP address. This is also known as link aggregation or trunking.

If you have implemented NIC teaming, but don't see load balancing working as expected, the problem may be resolved by configuring your switch to disable **flowcontrol send**. To do this, use the command `set port flowcontrol send off` for both the **port-channel** and **channel member** ports.

An anti-spoofing mechanism has been used in the switch

Network Agent uses spoofing to serve block messages. To use Network Agent, therefore, the anti-spoofing mechanism in the switch must be disabled. If this is not possible, Forcepoint URL Filtering customers may instead use a third-party integration product. For Forcepoint Web Security, this issue does not affect the Content Gateway proxy.

Can a network tap be used with Network Agent?

Yes. A tap can be used with the Network Agent machine. Network Agent must be able to see the traffic in both directions.

Published 06 August 2024