FORCEPOINT

Deploying an I Series Appliance

Forcepoint Web Security Cloud

2022

Last updated: May 13, 2022

Contents

1 Introduction

Deploying an I Series Appliance | Forcepoint Web Security Cloud

This guide describes deploying an I Series appliance as part of your Forcepoint Web Security Cloud solution.

The I Series appliance is an add-on to Forcepoint Web Security Cloud, providing fast on-premises URL analysis and application/protocol detection for web traffic, along with centralized policy management and reporting capabilities in the cloud. When a policy indicates that a request requires additional analysis, it is transparently routed to the cloud, where cloud analytics are applied and policy is enforced.

You can choose to deploy an appliance for all of your web traffic, or as part of a larger solution that combines the different management options available. For example, you may wish to have an appliance on one site, but deploy the PAC file for end users on another site, and install a web endpoint client for roaming users.

For information on getting started with the cloud service, including details of other deployment options, see the Forcepoint Web Security Cloud - Getting Started Guide.

Note

The data security features in Forcepoint Web Security Cloud are not currently supported with I Series appliances.

Once you have a cloud service account and have either received your I Series appliance or downloaded the appliance virtual image, you can deploy your appliance by completing the following tasks:

1. *Issues to consider before you begin*
2. *Initial portal settings*
3. *Setup and configuration*
4. *Connecting the appliance to your network*
5. *Registering the appliance*

The Quick Start poster, which is packaged in the appliance shipping box, outlines these tasks for your hardware version and includes a section for writing down reference information during deployment.

Recommendations for an evaluation

During the initial stages of an evaluation, it is recommended that you configure all of your IP address ranges as trusted network sources, meaning that the appliance ignores all traffic. You can then test your deployment with a small number of clients before opening it up to all IP addresses and ignoring only those addresses whose traffic you do not want to be analyzed (for example, servers that receive Microsoft and antivirus updates).

Issues to consider before you begin

Deploying an I Series Appliance | Forcepoint Web Security Cloud

Consider the following before you begin the deployment:

- If you have a hardware appliance, determine appliance rack location.
- If you are installing the appliance as a virtual machine, ensure the installation machine meets the following requirements:
  - For a Silicom bypass card deployment, the card should be installed on ESXi in VMDirectPath mode. For more information on Silicom card installation, see *Silicom card setup*, page 15.
  - 6 dedicated CPU cores and at least 12 GB RAM
  - 128 GB hard disk drive
  - The appliance virtual machine can be installed only on VMware vSphere ESXi 5.1, 5.5, or 6.0.
- Determine appliance IP addresses for network deployment. You will require 2 addresses, and it is recommended that you configure 3.
- Determine your directory synchronization policy.
- If you wish to use transparent NTLM authentication for your users, decide whether to connect your appliance to a local Active Directory (see *Configuring Active Directory authentication*, page 33).

  If you plan to use Active Directory authentication, ensure that your appliance hostname complies with Active Directory hostname requirements (see *First-Time Configuration Wizard*, page 24).

  Alternatively you can enter the domain that forms part of your users' NTLM identity when adding your appliance in the Forcepoint Cloud Security Gateway Portal, also referred to as the cloud portal.

Note

To use your Active Directory for authentication, the appliance must be able to access the directory's IP address and ports. You may need to edit an internal firewall setting or LAN routing rules.

- It is recommended that you provide a certificate when you add an appliance in the cloud portal, in order to avoid browser warnings regarding SSL termination for block, authentication, or quota/confirm operations. See *Generating an appliance certificate*, page 10.

  To use the cloud service SSL decryption feature, you must also install the Forcepoint root certificate on each client machine. See Enabling SSL decryption in the cloud portal Help.

- The appliance ships with a pre-installed category database. After appliance setup, an update to this database is initiated. During this update, the appliance can analyze traffic using the pre-installed database. Because this database is out-of-date, expect traffic analysis to become more accurate after the full update is complete.

  A progress message displayed on the **Status > General** page disappears when the update is complete.

- Browsing with Forcepoint Web Security Cloud via an I Series appliance has been tested with most commercially available web browsers. However, note that using a Windows XP machine with Internet Explorer 8 or below is not recommended, as HTTPS connections are not supported on I Series appliances for this platform and browser. For details of the supported browsers for use with the cloud service, see the article Forcepoint Cloud Security Browser Support Matrix in the Forcepoint Knowledge Base.

Using Forcepoint Web Security Endpoint with an appliance

Deploying an I Series Appliance | Forcepoint Web Security Cloud

If some of your end users have the Proxy Connect Forcepoint Web Security Endpoint installed, perhaps because they work remotely, you can set up your appliance to handle endpoint traffic in one of the following ways when those end users are at a site served by an appliance:

- Ignore all traffic generated by an endpoint client. This means that endpoint users are effectively treated as roaming users even when on-site.
- Manipulate PAC file requests from endpoint clients and ensure that endpoint traffic goes direct through the appliance rather than via the cloud service proxy. This means that end users have less latency and get a better user experience.

Both of these configurations must be enabled by Forcepoint. Please contact Forcepoint Technical Support for further information.

The Direct Connect Forcepoint Web Security Endpoint does not currently analyze browsing that takes place behind appliances.

2 Initial portal settings

You should have received your Forcepoint Web Security Cloud confirmation email, including a portal user name and temporary password if you are a new cloud services customer, as described in the Forcepoint Web Security Cloud Getting Started Guide. The initial setup involves the following tasks:

1. *Run directory synchronization*
2. *Add new appliance information*.

Run directory synchronization

It is recommended that you use directory synchronization to import user and group information from your LDAP directory (for example, Active Directory) into the portal. This is the quickest and easiest way to import end users' email addresses, as well as NTLM details if you are planning to use NTLM identification.

Note

For alternatives to directory synchronization, see Forcepoint Web Security Cloud - Getting Started Guide.

Forcepoint Web Security Cloud synchronizes with LDAP directories via a client-resident application called the Directory Synchronization Client. Changes made to a directory, such as deleting a former employee or adding a new one, are picked up by the service on the next scheduled update. If you have more than one LDAP directory, the client can merge them together before synchronizing the data with the service.

To set up and run directory synchronization:

1. Log on to the cloud portal from the machine you want to use for directory synchronization.
2. Go to the **Account > Directory Synchronization** page.
3. Download and install the appropriate version of the Directory Synchronization Client.

4. In the cloud portal, go to the **Account > Contacts** page and set up an administrator contact with Directory Synchronization permissions. The logon credentials you define will be used by the Directory Synchronization Client to log onto the manager.
5. Configure the Directory Synchronization Client as described in the *Directory Synchronization Client Administrator's Guide*, including the logon credentials you created in the previous step.

Note

If your LDAP data does not include users' email addresses, you can change the default attribute for the primary mail value in the Directory Synchronization Client as follows:

- When creating or modifying the Users part of your configuration profile, go to the **Data source > LDAP** search page in the wizard. Click **Advanced** to display the Search attributes page.
- In the Primary Mail field, replace %mail% with another attribute.

  For example, you could use %userPrincipalName% if configured, or create a 'fake' email address using the sAMAccountName such as %sAMAccountName%@mydomain.com.

6. Once you are ready to synchronize data with the cloud, go back to the **Account > Directory Synchronization** page.
   a. Click **Edit**.
   b. Click **Enable directory synchronization**.
   c. For **User policy assignment**, select Fixed.
   d. For **Email new users**, define whether synchronized users should receive a notification email from Forcepoint Web Security Cloud.
   e. Click **Submit** when done.
7. Run the synchronization, and check the results both in the client and on the portal:
   - In the client, click on the **Groups** and **Users** tabs to view the results.
   - On the portal, go to the **Account > Directory Synchronization** page. The Recent Synchronizations section shows your recent synchronization history; click the timestamp in the date column to view details about a specific synchronization.

Add new appliance information

Deploying an I Series Appliance | Forcepoint Web Security Cloud

To add your new appliance information in the portal:

1. Go to the **Web > Network Devices > Device Management** page.
2. Click the **New** button above the table, then click **Add Appliance**.

You are taken to the **Add Appliance** page.

Define general settings

Under **General Settings**:

1. Use the toggle at the top of the page to indicate whether this appliance is used for filtering (**ON** is the default). When filtering is set to OFF, the appliance can communicate with the cloud service, but allows all web traffic to pass through unfiltered.
2. Enter a unique appliance **Name** (1 - 512 alphanumeric characters) and **Description** (maximum length 1024 characters).
3. Select a **Default policy** for this appliance, and the **Time zone** used to apply policy settings.

   You will have a chance to apply different policies to different internal networks managed by this appliance later.
4. If you are using transparent NTLM authentication and your appliance is not connected to a local Active Directory instance, enter the **Authentication domain** that forms part of your users' NTLM identity. The NTLM domain is the first part of the domain\username with which users log on to their Windows PC; for example, MYDOMAIN\jsmith.

Important

You must configure your end users' browsers to support transparent NTLM authentication, either manually or via GPO or similar. See *Configuring browsers for NTLM identification*, page 37.

   If you have connected your appliance to a local Active Directory for NTLM authentication, this field is not required because the appliance automatically retrieves domain information from the local directory.
5. Select a time period after which a user's login and password must be revalidated from the **Session timeout** drop-down list. The default is 1 day.
6. **Forward traffic to the cloud for advanced analysis** is selected by default. This redirects appropriate traffic to the nearest cloud service data center for additional analysis. Clear this check box if you do not want any traffic to be forwarded to the cloud. All traffic will be analyzed through the appliance, without any cloud analytics.

Configure a Certificate Authority

Under **Certificate Authority**:

1. Use the drop-down list to indicate whether to **Upload certificate files**, or **Use default certificate**.

Important

Forcepoint recommends that you define certificates when you add an appliance, in order to avoid browser warnings regarding SSL termination block, authentication, or quota/confirm operations. Some browsers, for example later versions of Chrome, may block the transaction and display an error message.

Be sure to:

1. Generate a CA certificate. Each appliance should have a valid X.509 identity certificate with an unencrypted key. This certificate can be generated using a variety of tools, for example OpenSSL. For details and an example, see *Generating an appliance certificate*, page 10.
2. Import this certificate to all relevant browsers.
3. Upload this certificate to each appliance as described below.

To use the cloud service SSL decryption feature, you must also install the Forcepoint root certificate on each client machine. See Enabling SSL decryption in the cloud portal Help.

2. If you have selected to upload certificate files, click **Browse** to navigate to the public certificate file, then click **Open** to populate the **Public certificate** field.
3. Next, click **Browse** to navigate to the private key file, then click **Open** to populate the **Private key** field. The private key must be in either PEM or .key format.
4. If you have chained certificates, click **Browse** and navigate to the intermediate certificate, then click **Open** to populate the **Chained certificate** field.

   The certificate chain should include the root CA, and optionally additional intermediate CAs.

Generating an appliance certificate

Deploying an I Series Appliance | Forcepoint Web Security Cloud

Each appliance should have a valid X.509 version 3 identity certificate in PEM format with an unencrypted key. This certificate can be generated using a variety of tools. Below is a simple procedure using OpenSSL to generate a private key and CA that can be used for your appliance.

This section assumes that you are familiar with OpenSSL and have a working OpenSSL installation.

The following OpenSSL statement creates a 2048-bit RSA private key with a password of 1234:

```
openssl genrsa -passout pass:1234 -des3 -out
CA_key_password.pem 2048
```

You must supply a password, as OpenSSL does not allow the creation of a private key without one. You can then strip the password from the key as follows:

```
openssl rsa -in CA_key_password.pem -passin pass:1234 -out
CA_key.pem
```

This also renames the private key file from CA_key_password.pem to CA_key.pem.

Finally, use the following statement to create the CA:

```
openssl req -x509 -days 11000 -new -sha1 -key CA_key.pem -
out CA_cert.pem
```

Note that this command prompts you to input information about different parameters, such as country, state, locality, or your organization's name.

Once you have created the private key (CA_key.pem) and public certificate (CA_cert.pem), import the certificate to all relevant browsers, and upload the certificate to each appliance using the Certificates tab.

Define internal network settings

The Internal Networks section of the page is used to optionally:

- Assign different policies to different internal networks.
- Identify trusted networks for which incoming or outgoing traffic, or both, should not be analyzed.
- Configure session-based authentication for specific networks.

To begin:

1. Select the **Policy Assignment** tab and click **Add** to identify a network to which you want to assign a policy other than the appliance default. In the **Add Policy Assignment** dialog box:
   a. Enter a unique **Name** for the network.
   b. Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).
   c. Enter the subnet, address, or range.
   d. Select a **Policy** from the drop-down list.
   e. Click **Add**.

   Repeat these steps for each internal network to which you want to assign a policy.

   Note that networks (IP address ranges and subnets) may not overlap, and you can assign only one policy to each network.
2. Select the **Trusted Networks** tab and click **Add** to identify IP addresses or address ranges whose traffic should not be analyzed. In the **Add Trusted Network** dialog box:
   a. Enter a unique **Name** for the network.

b. Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).

c. Enter the subnet, address, or range.

d. Indicate whether to **Bypass analysis for traffic from this network**, **Bypass analysis for traffic to this network**, or both.

e. Click **Add**.

Repeat these steps for each internal network whose incoming or outgoing traffic, or both, should not be analyzed.

3. Select the **Session-Based Authentication** tab and click **Add** to define network addresses and IP address ranges that should use session-based authentication. The defined addresses will be authenticated based on a cookie sent to the browser on the local machine.

   This authentication is valid for the length of time defined in the **Session timeout** drop-down list (under General).

   a. Enter a unique **Name** for the network.

   b. Use the **Type** list to indicate how you want to identify the network (IP address, Subnet, or IP range).

   c. Enter the subnet, address, or range.

   d. Click **Add**.

   Repeat these steps for each internal network that will use session-based authentication.

Note

When session-based authentication is enabled, policy SSL decryption rules that apply to sites or categories with the Confirm action are not currently supported.

3 Setup and configuration

Perform the steps below to set up and configure your appliance. The steps for the hardware version are also described, with diagrams, on the Quick Start poster.

1. Either:
   - Verify the contents of the accessory box that was shipped with the appliance. It should include power cable, an appliance bezel, and a quick start poster on the Forcepoint Documentation website.
   - Rack the appliance and plug it in.

   Or:
   - Deploy the I Series appliance OVA file on a VMware ESXi workstation server. See *Installing the appliance on a virtual machine*, page 13.
2. Power the appliance on and allow the boot sequence to complete.
3. Connect a computer with DHCP enabled (such as a laptop) to the appliance C1 interface. Wait a few moments, until the automatic network setup process is complete, to begin appliance configuration.
4. Log on to the appliance via a web browser connection (https://169.254.0.2). Credentials are admin/admin.
5. Complete the appliance *First-Time Configuration Wizard*.
6. Log off the appliance and disconnect the computer from the appliance.

Installing the appliance on a virtual machine

Download the OVA file suitable for your deployment from your website account to a local directory. There are 2 ways to install appliance on a virtual machine:

- With a Silicom bypass card connected to the ESXi host, and with one management NIC. For this scenario, use the OVA file starting **Websense-i500v-dio-bp-InstallImage**.
- Without a Silicom card, just using 3 virtual switches. In this scenario, use the OVA file starting **Websense-i500v-InstallImage**.

Ensure the installation machine meets the following requirements:

- For a Silicom bypass card deployment, the card should be installed on ESXi in VMDirectPath mode. For more information on Silicom card installation, see *Silicom card setup*, page 15.
- 6 dedicated CPU cores and at least 12 GB RAM
- 128 GB hard disk drive
- The appliance virtual machine can be installed only on VMware vSphere ESXi 5.1, 5.5, or 6.0.

This section describes how to set up the ESXi machine, and how to install the OVA file.

Network settings

It is recommended that you have dedicated NICs for each of the 3 switches required for the appliance. The B1 WAN and B2 LAN switches must use different physical interfaces.

Important

Do not use the ESXi management physical interface for the B1 or B2 switch.

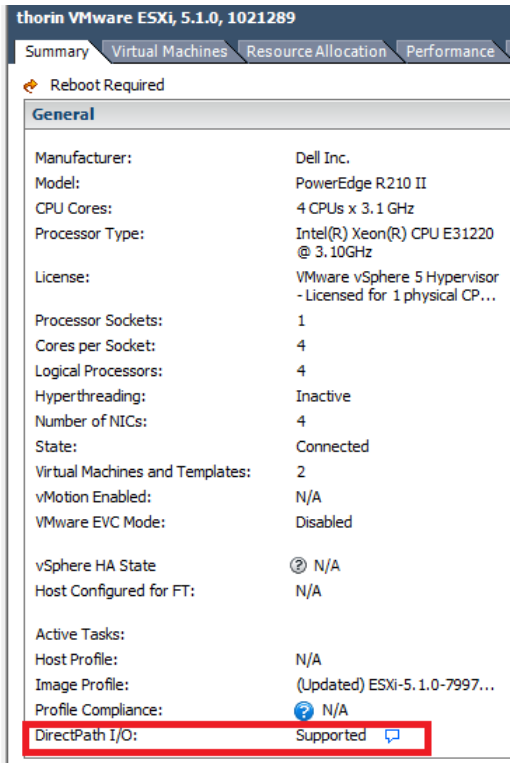
To create the required network interfaces:

1. In the VMware vSphere Client, select **Hosts and Clusters**.
2. Select your host and click the **Configuration** tab.
3. Select **Networking** in the **Hardware** section, and click **Add Networking**.
4. Select a connection type and click **Next**.
5. Select **Create a vSphere standard switch**.
6. Select the check boxes for the network adapters that your standard switch will use and click **Next**.
7. Under Port Group Properties, enter a network label for the management NIC: C1 Management.
8. Click **Next**.
9. Review your settings and click **Finish**.

10. Repeat these steps for 2 more switches: B1 WAN (for outgoing traffic) and B2 LAN (for incoming traffic).

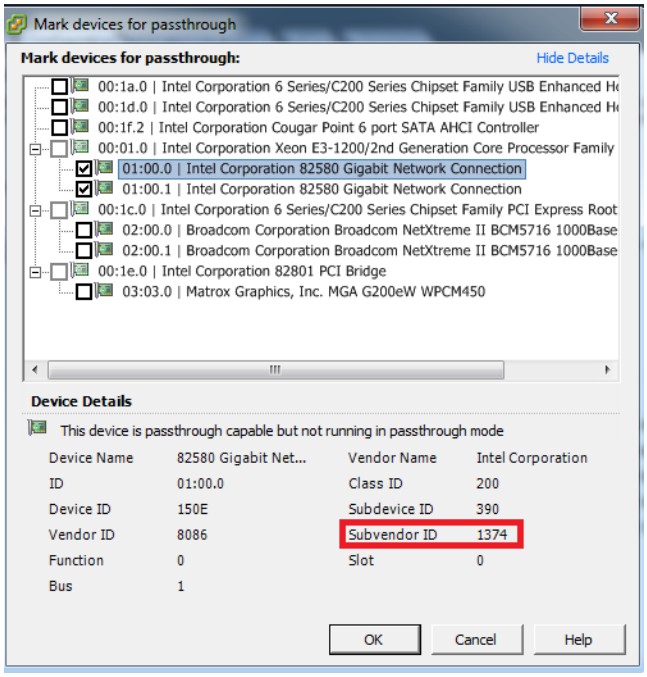
Silicom card setup

To set up the Silicom bypass card on the ESXi machine, VMDirectPath technology is required. To use VMDirectPath, verify that the host has Intel® Virtualization Technology for Directed I/O (VT-d) or AMD I/O Virtualization Technology (IOMMU) enabled in the BIOS.



1. In the vSphere Client, go to the **Configuration** tab and select **Advanced Settings** in the **Hardware** section.
2. Click the **Edit** link.

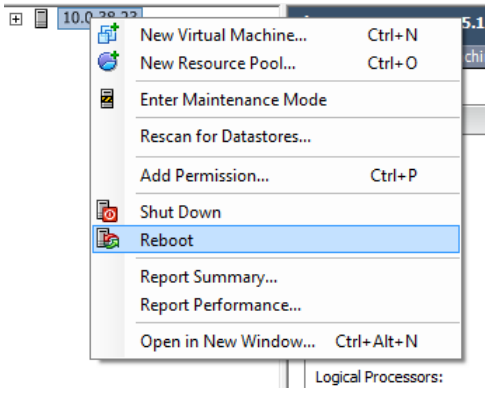
3. Mark the Silicom card check box. You can identify the Silicom card by checking the device details for the Silicom Subvendor ID, which should be 1374.



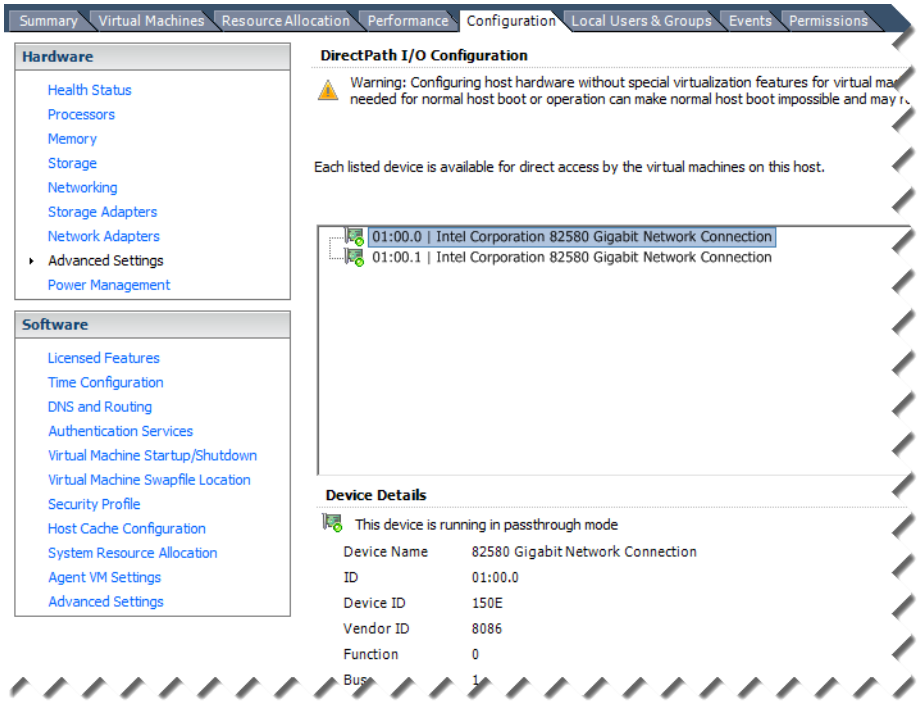
4. Click **OK**.

   The message “Changes made to some of the devices below will not take effect until the host is restarted” appears on the Advanced Settings screen.

5. Restart the ESXi host server.



After the restart, the list of Silicom Card NICs should appear on the Advanced Settings screen with green bullets.

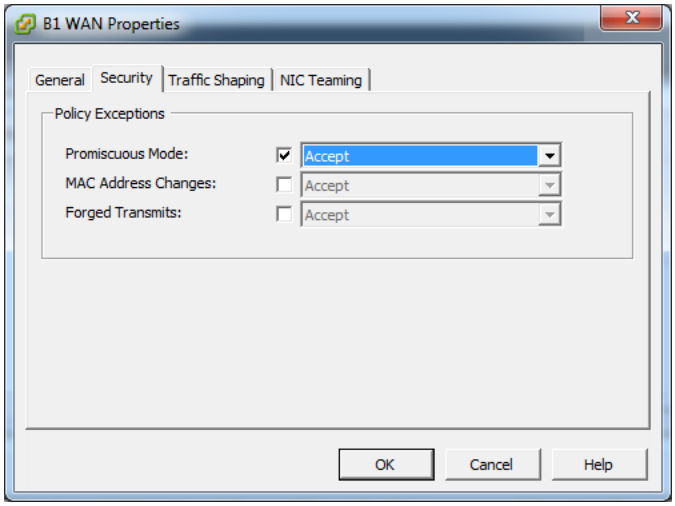


Setting up promiscuous mode (no Silicom card)

If you are installing without a Silicom card, you must set the B1 and B2 NICs to be in promiscuous mode:

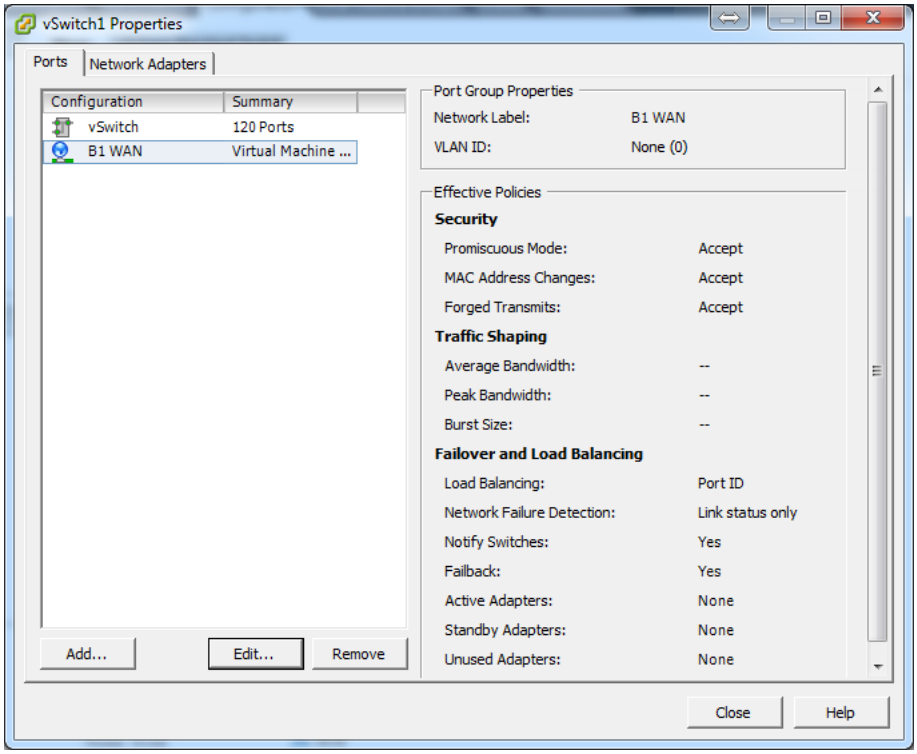
1. In the vSphere Client, go to the **Configuration** tab and select **Networking** in the **Hardware** section.
2. Click the **Properties** link for the B1 switch.
3. Select the B1 NIC in the list, then click **Edit**.

4. On the Security tab, mark **Promiscuous Mode**, and select Accept from the drop-down list.



Click **OK**.

5. The B1 NIC properties should now look like this:



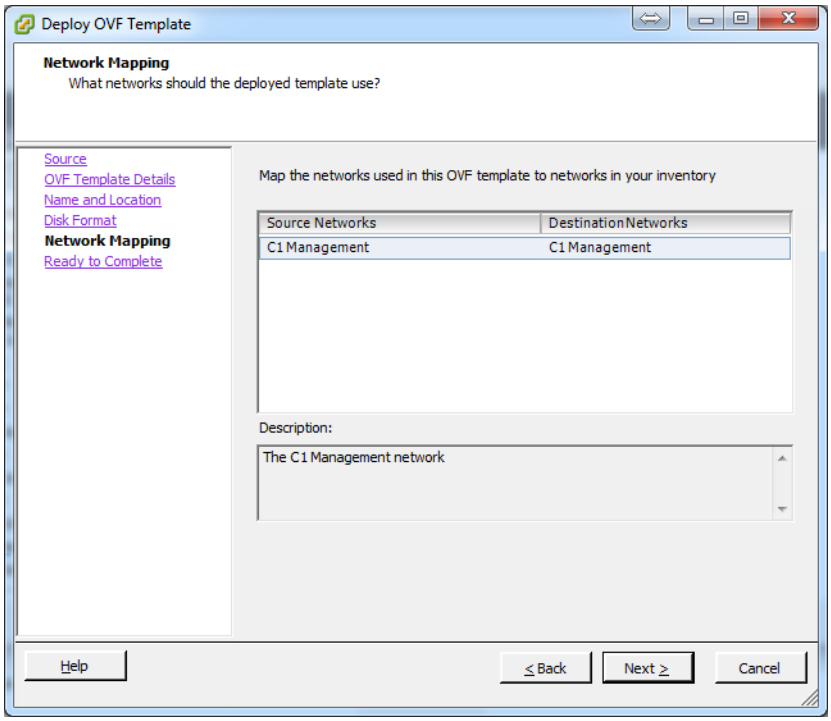
Click **Close**.

6. Repeat steps 2-5 for the B2 NIC.

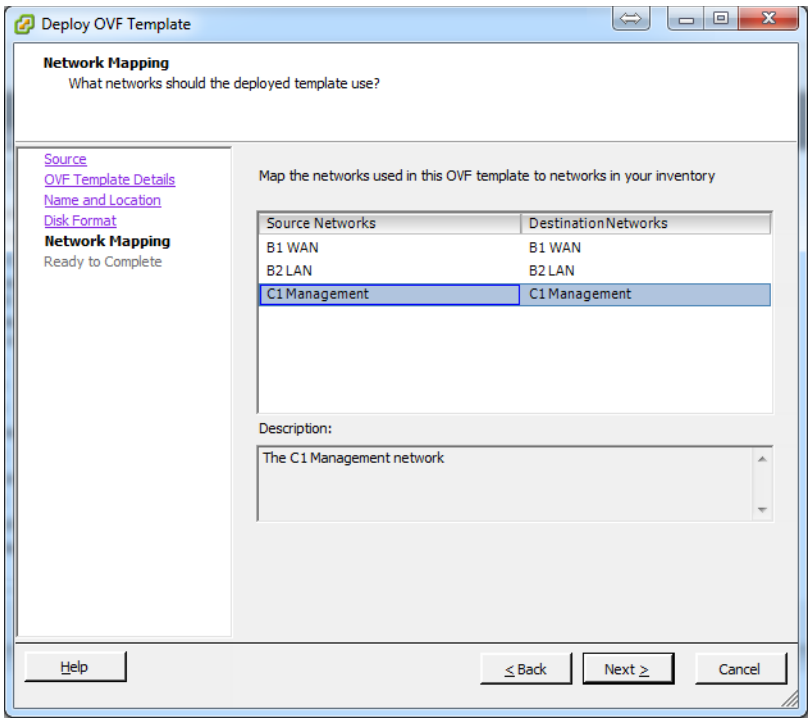
Importing the OVA

1. In the vSphere Client, go to **File > Deploy OVF Template**.
2. Browse to the OVA file that you downloaded from your Forcepoint website account, then click **Next** twice.
3. Enter a name for the I Series appliance VM, then click **Next** twice.
4. If you set up the network configuration on the ESXi host as described in *Network settings*, you should see the following screen:

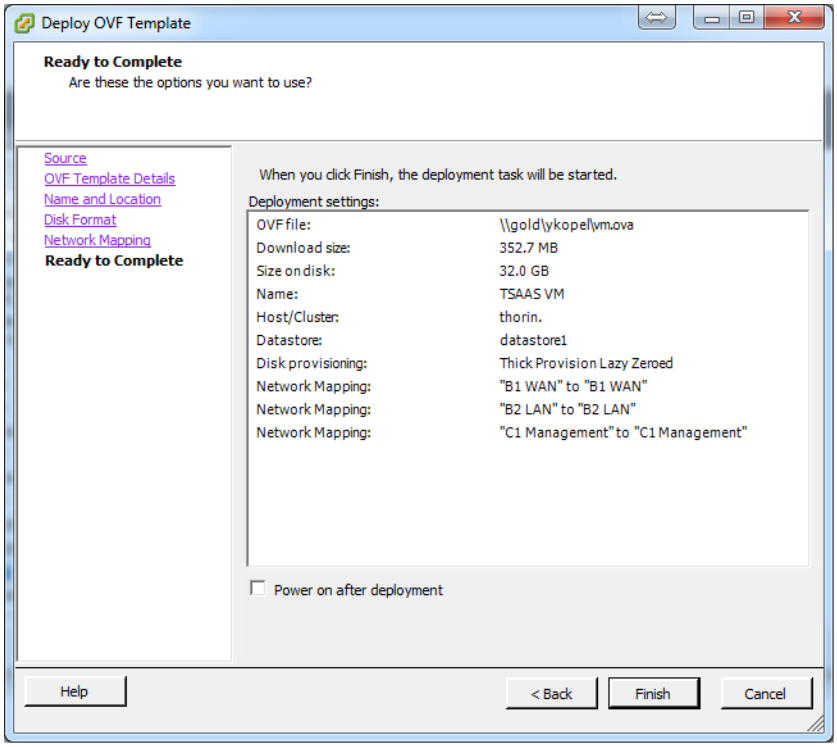
   For a VM with Silicom card:



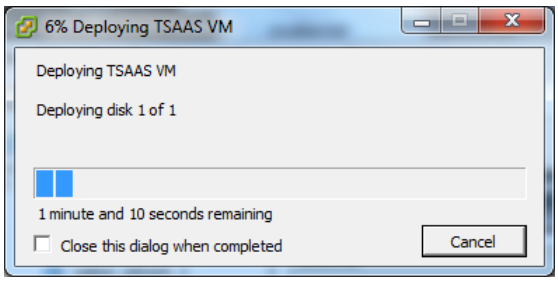
For a VM without Silicom card:



5. Click **Next**.



6. Click **Finish**, and wait for the installation to complete.



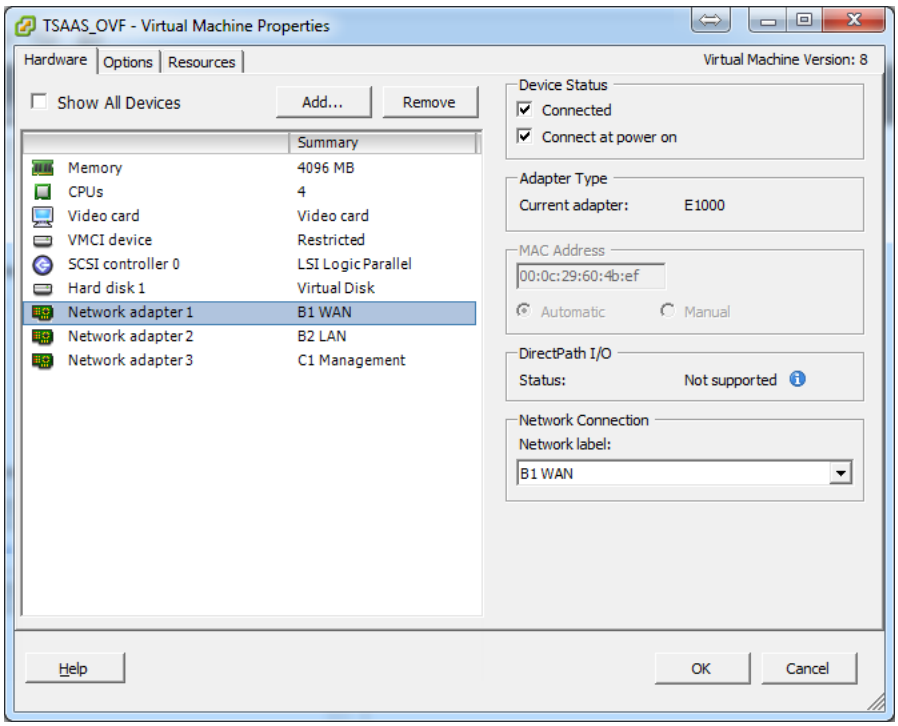
Deployment without Silicom card

Deploying an I Series Appliance | Forcepoint Web Security Cloud

If you have deployed the VM without a Silicom card, you must verify the MAC addresses that have been generated:

1. Initially, no MAC addresses are assigned to the machine NICs. Turn on the new VM, then right-click the VM and select **Edit Settings**.

   Each NIC should now have a MAC address:



2. Confirm that the generated MAC addresses are in alphabetical order, with B1 WAN having the lowest address, followed by B2 LAN and then C1 Management. If this is not the case, change the mapping of your NICs as follows:

   a. Select the NIC with the lowest MAC address.

   b. Under **Network Connection**, change the **Network label** to B1 WAN.

c. Repeat the **Network label** change for the next lowest MAC address (setting it to B2 LAN) and finally the highest MAC address (setting it to C1 Management).

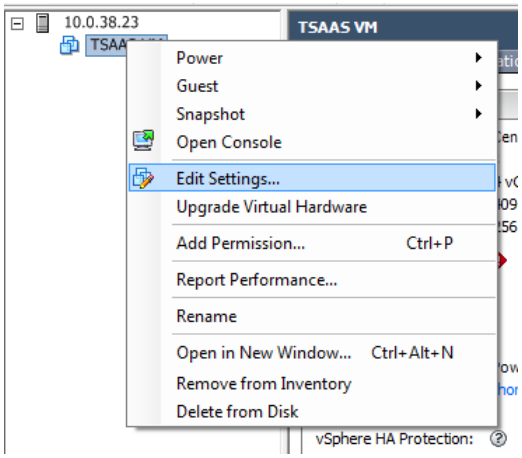
d. Click **OK** when done.

Deployment with Silicom card

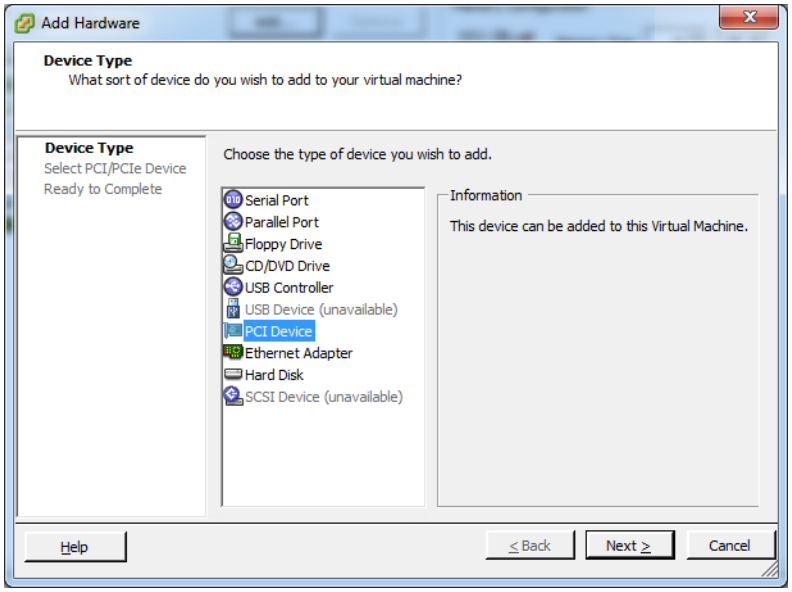
Deploying an I Series Appliance | Forcepoint Web Security Cloud

If you have deployed the VM with a Silicom card, you should connect the Silicom Card NICs to the new VM as follows:

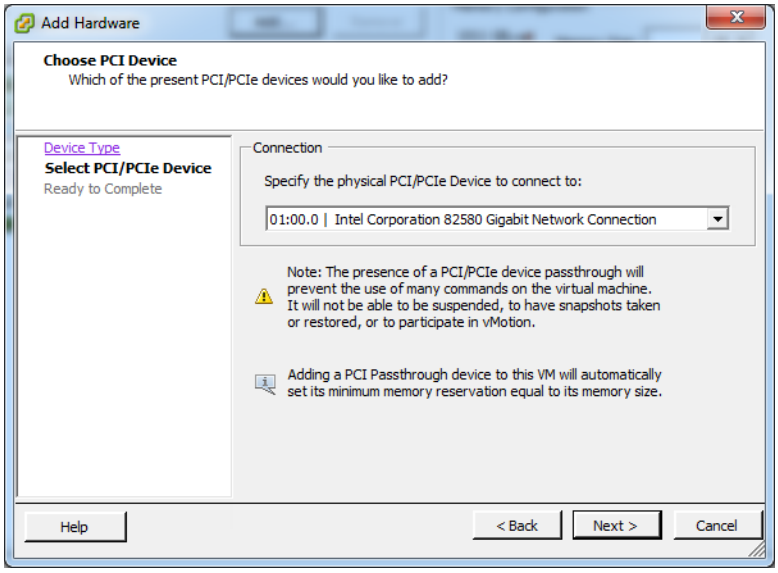
1. Right-click the new VM, and select **Edit Settings**.

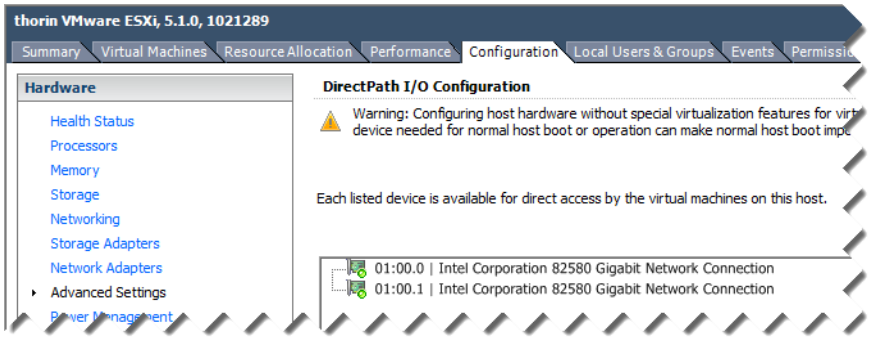


2. Click **Add**.
3. Select PCI Device from the **Device Type** list, then click **Next**.



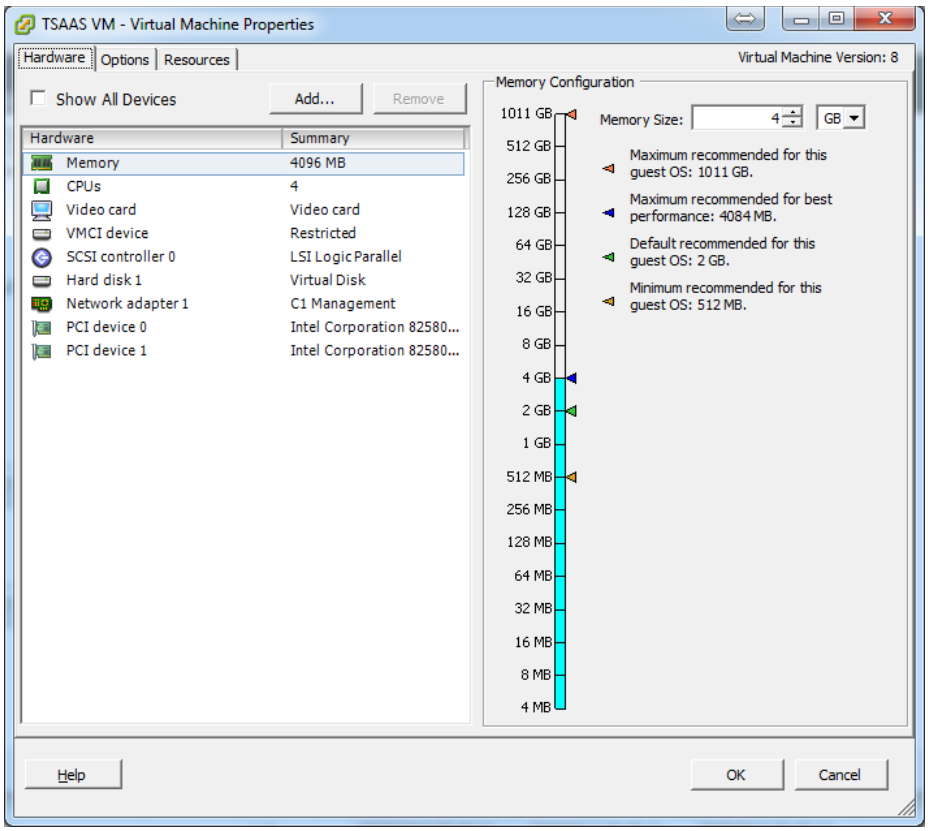
4. Choose the first NIC of the Silicom card (this is the first entry displayed on the **Configuration** tab > **Advanced Settings** page).





5. Click **Next**, then click **Finish**.
6. Repeat steps 2-5 for the second Silicom NIC.

7. Click **OK** on the Virtual Machine Properties page to see the final result:



First-Time Configuration Wizard

Deploying an I Series Appliance | Forcepoint Web Security Cloud

The First-Time Configuration Wizard walks you through some initial settings that are important for appliance operation. You must complete the wizard before you can manage the appliance. Canceling the wizard before completing initial appliance configuration logs you out of the appliance, and any settings you may have entered up to that point are not saved.

Click **Next** on the Welcome page to start the wizard.

1. On the Hostname page, enter the appliance host name or fully-qualified domain name (FQDN). The name can consist of 1-32 alphanumeric characters, dashes, and periods. It must begin with a letter and cannot end with a period.

   The format for an appliance hostname is *hostname*. You can also use the format *hostname.parentdomain.*

   The format for the FQDN is *hostname.parentdomain.com.*

   If you plan to use Active Directory authentication, the following hostname requirements are enforced:

- Total length of 2 - 128 alphanumeric characters (including hostname and parent domain name elements; format is *hostname.parentdomain*)
- May include dashes, underscores, and periods
- Must begin with an alphanumeric character
- Cannot end with a dash, underscore, or period
- Hostname element length should be between 2 and 15 characters
- Cannot match any of the following reserved words:

ANONYMOUS	BATCH	BUILTIN
DIALUP	INTERACTIVE	INTERNET
LOCAL	NETWORK	NULL
PROXY	RESTRICTED	SELF
SERVER	SERVICE	SYSTEM
USERS	WORLD	

Click **Next** to continue with the wizard.

2. On the Network Interfaces page:
   a. In the Outbound Traffic section, specify the appliance IP address and subnet mask for the network bridge created by the B1 and B2 interfaces. These interfaces are used for all outbound traffic. One interface (B1) handles traffic routed out of your network, and the other (B2) handles traffic to your internal network.
   b. To allow appliance management via the B1 and B2 bridge interfaces along with the C1 interface, mark the **Allow appliance management access in addition to the C1 interface** check box.
   c. Provide the IP address and subnet mask for the C1 interface in the Appliance Management section. This interface is used for appliance management functions. This interface can also be used when the B1/B2 bridge interface is in hardware bypass mode.

      If you have deployed a virtual appliance that does not include the appliance bypass function, use of the C1 interface for appliance management is optional. If you do not define a C1 management interface, then you must use the B1/B2 bridge interface for management purposes. In this case, the Outbound Traffic section includes a **Use this interface for appliance management** check box, which is marked and not accessible.

      If you do wish to define a C1 management interface, mark the **Use a dedicated appliance management IP address** check box in the Optional Appliance Management section, and enter the IP address and subnet mask for the C1 interface. The **Allow appliance management access in addition to the C1 interface** check box is then accessible for marking or clearing.
   d. In the DNS Servers section, define a DNS server by entering its IP address in the **IP address** field and clicking **Add**. The IP address appears in the DNS Server IP Address list.

You can define up to 3 DNS servers. You cannot define more than one server with the same IP address.

Click **Next** to continue with the wizard.

3. On the Routing page, specify the IP address of your default gateway for outbound traffic.

Note

In many cases, you need only a gateway specification on this page. However, there may be cases where explicit or static routing is required. For more information on these scenarios, please see the knowledge article Configuring routing for I Series appliances.

If you need to define routing over the bridge interface, please contact Technical Support in the first instance. You can define routing rules over the management interface as follows:

Click **Routing Table**.

Click **Add** and then provide the following route information in the Route Properties dialog box:

- Destination network
- Subnet mask for the destination network
- Gateway IP address
- Interface used. In the drop-down list, select either **Bridge, (B1, B2)** or **Management (C1)**.

The appliance supports the use of a single VLAN tag to identify management communication traffic from the appliance to the cloud and database download services. This tag is also used by any client that communicates with the appliance bridge interface, either explicitly for management purposes or transparently, for example for authentication, or for quota or confirm actions when filtering.

Note

Ensure you have configured valid routing between any client generating traffic that is intercepted by the appliance and the bridge interface, taking into account the VLAN tag that you define on this page.

Mark the **Use the following VLAN tag** check box, then enter the tag in the entry field using a number from 0 to 4094.

Click **Next** to continue with the wizard.

4. The final page of the wizard summarizes the entries and selections you have made. If you want to change any setting after your review, click **Back** to access the desired wizard page and edit your settings.

   If you are satisfied with your settings, click **Finish**.

You must log off the appliance and log back on for your configuration settings to take effect.

When you log back on, you are prompted to change your initial password (if you have not already done so) and register the appliance with Forcepoint Web Security Cloud. See *Registering the appliance* for information.

Note

If you are unable to access the appliance, you can connect to the appliance manager interface at any time using the C1 interface via https://169.254.0.2.

4 Connecting and registering the appliance

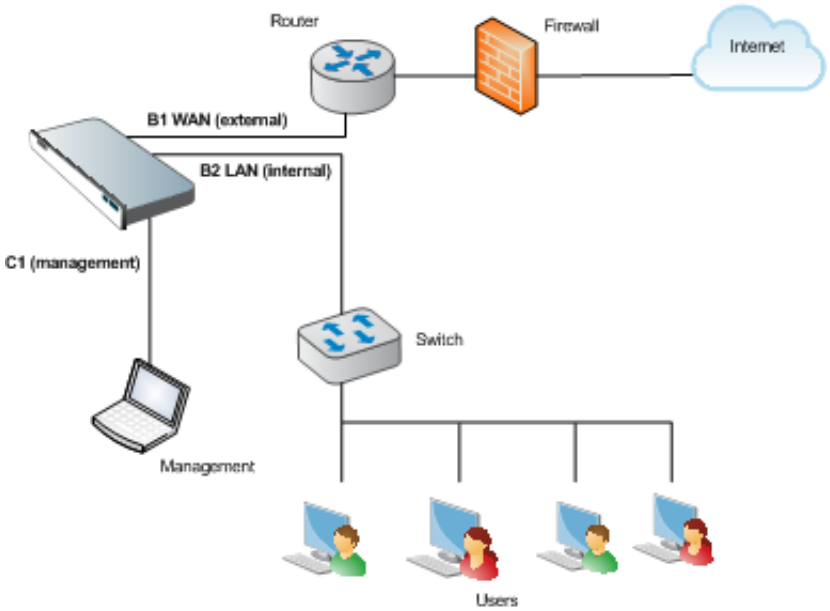
This chapter describes connecting the appliance to your network, and registering the appliance with the Forcepoint cloud service. It also contains information on running diagnostics, and monitoring appliance traffic.

Connecting the appliance to your network

Connect the appliance to your network. The appliance must have at least a valid connection to the cloud service for registration and the subsequent database update to succeed. You can choose either of the following methods:

- Install the appliance in your network and then register it with the cloud service. The appliance operates as a simple network bridge, forwarding all traffic, until registration is complete.
- Install the appliance offline, with only the B1 interface connected to the network to allow an upstream connection to the cloud service. Once registration is complete and the appliance is fully set up, you can connect it to your the rest of your network.

The sample diagram shows a typical deployment:



Configuring your firewall

Deploying an I Series Appliance | Forcepoint Web Security Cloud

If your network includes a firewall, by default your appliance is configured to use the standard destination TCP ports 80 and 443 for connections to the cloud service. Ensure these ports are open.

Alternatively and depending on your corporate firewall policy, you can configure your appliance to use the following ports, which are the ones used for non-appliance connections to the cloud service:

Port	Purpose
8002	**Configuration and policy update information retrieval from Forcepoint Web Security Cloud.** This port must be open for an I Series appliance to retrieve periodic configuration and policy updates from the cloud service.
8081	**Proxy service**. This is where the cloud-based content analysis is provided.

80	**Notification page components**. The default notification pages refer to style sheets and images served from the Forcepoint Web Security Cloud cloud platform. For these pages to appear correctly, this Web site is accessed directly (i.e., not through the cloud service). This port should also be opened for standard web traffic that does not need to be sent to the cloud for further analysis.
443	**Service administration**. The cloud portal is similarly unproxied. Otherwise, it would be possible for you to accidentally block access and then be unable to rectify the situation. This port should also be opened for standard secure web traffic that does not need to be sent to the cloud for further analysis, and for database updates.

You can switch between the standard and alternative ports at any time using the appliance command-line interface (CLI). To switch port settings:

1. On the appliance machine, open a command-line window.
2. Type **device**.

   ```
   cmd> device
   ```
3. Type one of the following:

   ```
   device> use_standard_ports yes
   ```

   for the standard ports 80 and 443

   ```
   device> use_standard_ports no
   ```

   for the alternative ports 8002 and 8081, plus 80 and 443

   The CLI returns the confirmation `Done` when the ports have been switched. If the ports are already set to the option you specify, the CLI returns `Not changed`.

You must also open outbound UDP port 123 to enable the appliance to synchronize its clock with the Network Time Protocol.

To guarantee availability, Forcepoint Web Security Cloud uses global load balancing technology to direct traffic across multiple geographic locations. Content analysis is typically always performed by proxies from the cloud service closest to the end user. In the event of localized or Internet-wide connectivity issues, the global load balancing technology automatically routes requests to the next closest location. To make the most of the resilience offered by this infrastructure, users must be allowed to connect to the entire cloud service network, both those IP addresses that the service uses now and those that may be deployed in the future.

If you decide to lock down your firewall, you should permit all the IP address ranges in use by the Forcepoint cloud service for all the above ports. These ranges are published in the Knowledge Base article Cloud service data center IP addresses and port numbers. Note that you must log on to your Forcepoint support account to view this article.

Registering the appliance

Once you have connected the appliance to your network, change the initial password and register the appliance with Forcepoint Web Security Cloud.

When you log back in to the appliance after completing the First-Time Configuration Wizard, the initial screen lets you change the initial password, if you have not already done so, in the Administrator Credentials box. If you changed the password before completing the wizard, the Administrator Credentials box does not appear on this page when you log back in.

This initial page also lets you enter your Forcepoint Web Security Cloud registration key. To register your appliance:

1. Log on to the cloud portal and select **Web > Network Devices**.
2. Select the row that contains this appliance.
3. Click **Register** at the bottom of the page to open the Register Appliance box.
4. Copy the displayed registration key and click **Close**.
5. Return to the appliance manager and paste the key into the **Registration key** field.
6. Click **OK**.

At this point, an update to the pre-installed Web category database begins. During this update, the appliance can analyze traffic using the pre-installed database. Note that this database is out-of-date, and analysis may be more accurate after the update process completes.

A download progress message appears on the **Status > General** page. This message disappears when the update is complete.

5 Next steps

Now you have completed the initial setup process, you can begin configuring your service to manage your organization's traffic. To get started with the cloud portal, refer to the Forcepoint Web Security Cloud Getting Started Guide.

Additional information and help for your appliance hardware version can be found on the Forcepoint Documentation website.

This chapter contains guidance on using the following features of your I Series appliance:

- *Configuring Active Directory authentication*
- *Managing protocols and exceptions*
- *Running diagnostics*
- *Monitoring appliance traffic*

Configuring Active Directory authentication

Use the appliance **Configuration > System** page to connect to an Active Directory server for transparent NTLM authentication. When this screen first opens, the status under Active Directory Authentication is **Disconnected**, and a button labeled **Connect** is available.

To establish a connection to an Active Directory server for authentication:

1. Click **Connect**.
2. In the Active Directory Authentication dialog, enter the following server information in the appropriate fields:
   - Domain name
   - Active Directory administrator name
   - Active Directory administrator password

     Note that this password is used only for establishing the server connection. The contents of this field are not stored anywhere in the system.
3. Indicate how the system finds the domain controller by selecting 1 of the following options:

- Auto-detect using DNS
- Enter a domain controller name or IP address.

  You can specify backup servers in a comma-separated list.

4. Click **OK**.

The connection cannot be made if the server hostname does not adhere to Active Directory naming restrictions. See *First-Time Configuration Wizard*, page 24, for a detailed list of Active Directory hostname requirements.

After a connection is successfully established, the button name changes from **Connect** to **Disconnect**.

Enabling browsers for NTLM transparent authentication

In an I Series appliance deployment, NTLM transparent authentication is available for your end users if you:

- Connect your appliance to a local Active Directory
- Enter your NTLM domain on the Authentication tab when you add your appliance to Forcepoint Web Security Cloud
- Select NTLM transparent identification where possible on the Access Control tab in your Forcepoint Web Security Cloud policy.

Note

If validating against a local Active Directory for NTLM authentication, an end user cannot use their email addresses as their user name, and must use the domain\username format (for example, MYCOMPANY\jsmith).

In order for a browser to work with NTLM transparent authentication, the machine on which the browser is hosted must be part of the domain. You must also configure your end users' browsers to support this form of authentication. See *Configuring browsers for NTLM identification*, page 37.

Managing protocols and exceptions

Deploying an I Series Appliance | Forcepoint Web Security Cloud

Protocols

Click the **Protocols** tab to manage how protocols, or non-HTTP Internet traffic, are handled by a policy.

The list of protocols appears in a 2-level tree display similar to that in the Categories tab. Protocol groups can be expanded to show the individual protocols within each group.

The list on the Protocols tab includes both standard protocols and any custom protocols that you have defined on the **Policy Management > Protocols** page. The standard protocol groups are updated regularly.

Configure how a protocol is filtered by selecting it in the protocols tree and specifying an action (**Allow** or **Block**) from the box on the right. You can select a protocol directly from the list, or enter text in the search box to locate the protocol you want.

Use the **Shift** and/or **Ctrl** keys to select multiple protocols.

Exceptions

Exceptions allow the default action for a protocol to be overridden for specified users and groups of users.

Exceptions are listed at the bottom of ther Protocols tab. You can click a protocol to view the exception rules that apply to it. Click **Add** to add a new exception.

For more information, see Exceptions in the Forcepoint Web Security Cloud help.

Running diagnostics

Deploying an I Series Appliance | Forcepoint Web Security Cloud

The Diagnostics tab on the appliance **Status > Alerts and Diagnostics** page provides the capability to run a series of system tests to determine the current state of the cloud service. As a best practice, it is recommended that you run these tests when you first deploy an appliance, and if you encounter any connectivity issues.

The first time you open the Diagnostics tab, a table shows a list of the tests to run. The tests include, for example, a status check of the network interfaces, the default gateway, your DNS servers, or the cloud connection.

Click **Run Diagnostics** to start the tests. The Results column displays test status (In progress) and results (Passed, Failed, or Could not complete). For tests that do not

complete or fail, the Details column displays more information, including suggestions for resolving the issue that caused the failure.

Each time you open the Diagnostics tab thereafter, the results of the last test run appear, along with the date/time of those tests.

Monitoring appliance traffic

The capability to monitor appliance traffic for troubleshooting purposes is available via the appliance command-line interface (CLI). Access the traffic monitor using the following commands:

```
cmd> status
status> monitor
```

Then run the monitor using the **monitor** command and its arguments:

```
monitor <arguments>
```

Other command options let you configure default display attributes for the log entries as well as display custom attribute combinations and protocols. Detailed information about the CLI monitor command options can be found in the document I Series Appliance Traffic Monitor.

A Configuring browsers for NTLM identification

This appendix describes how to configure supported Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox for NTLM transparent identification, either manually or via a Group Policy.

Internet Explorer & Google Chrome

Note

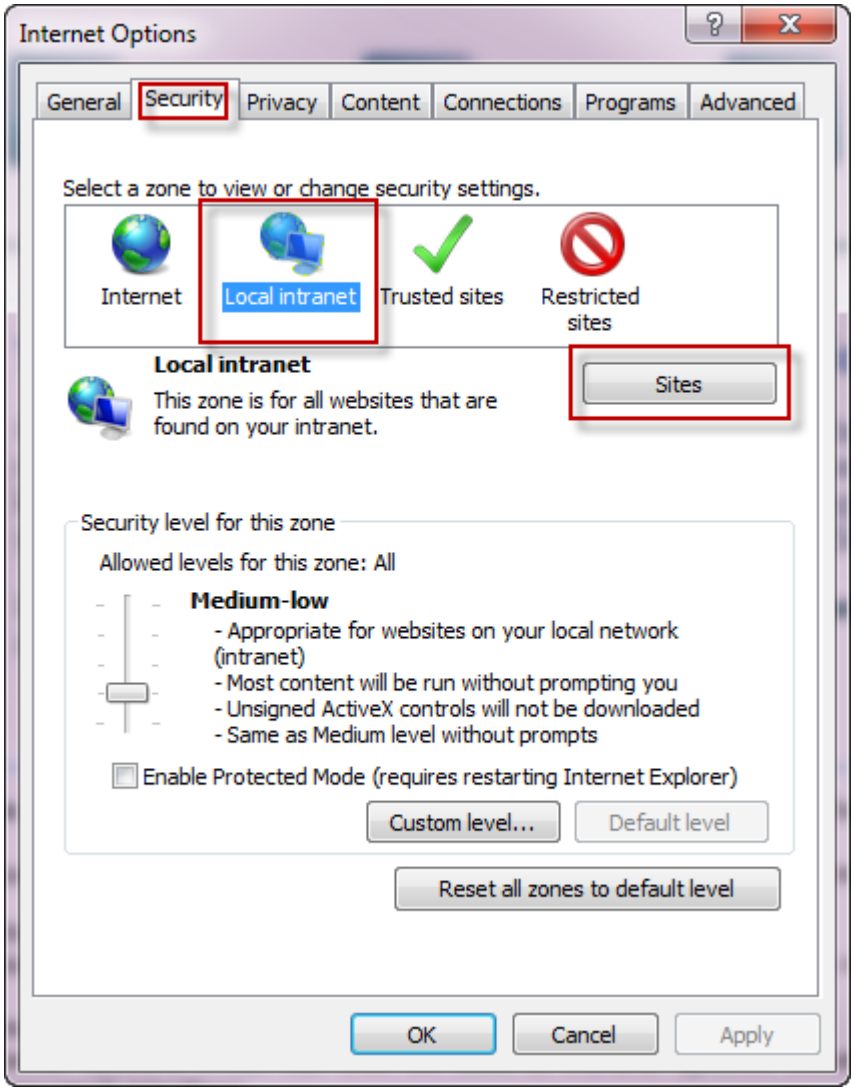
The settings in this section will also be applied to a Google Chrome browser on the same machine.

The screenshots in this section are taken from Internet Explorer 11 on Windows 7.

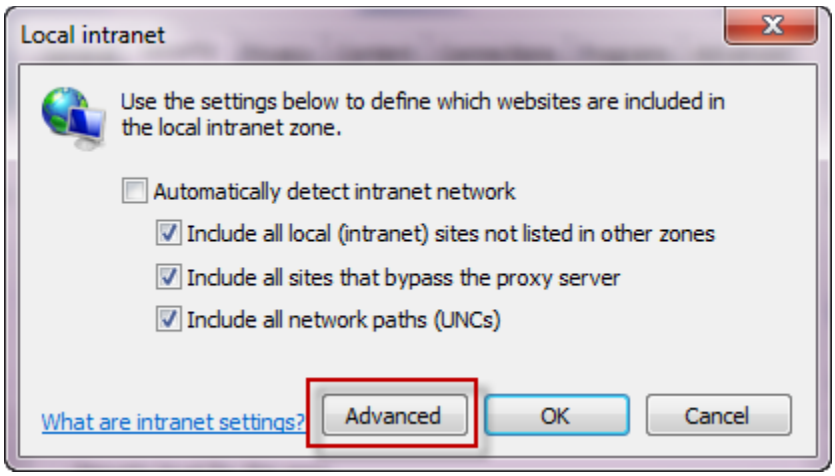
To enable NTLM on a single Internet Explorer browser:

1. Go to **Tools > Internet Options**.
2. Select the **Security** tab.

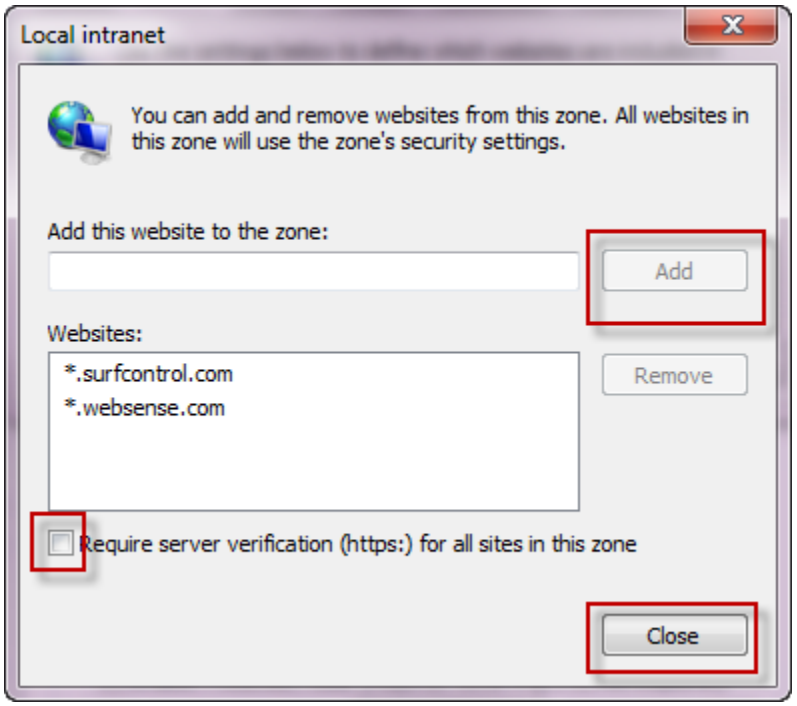
3. Select **Local Intranet**, then click **Sites** to open the list of Trusted Sites for the Intranet zone.



4. For Internet Explorer 8 and above, click **Advanced** on the window that appears.

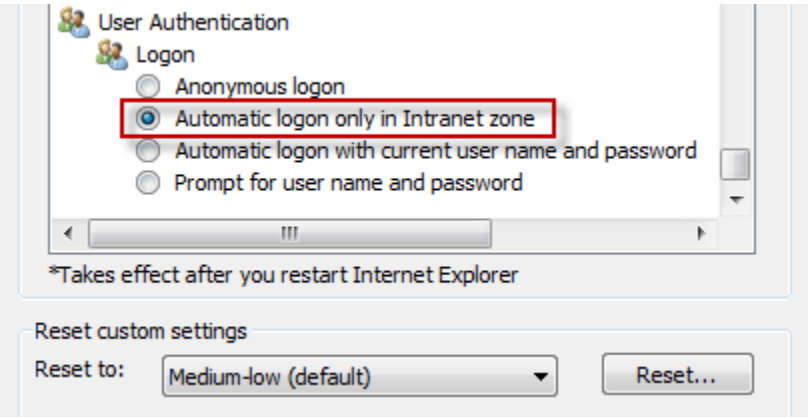


5. Enter the IP address of the B1/B2 bridge interface on your appliance, then click **Add**.
6. Clear the **Require server verification** box.
7. Click **Close**.



8. With Local Intranet still selected, click **Custom level**.

9. Scroll down to the User Authentication section, and ensure **Automatic logon only in Intranet zone** is selected.

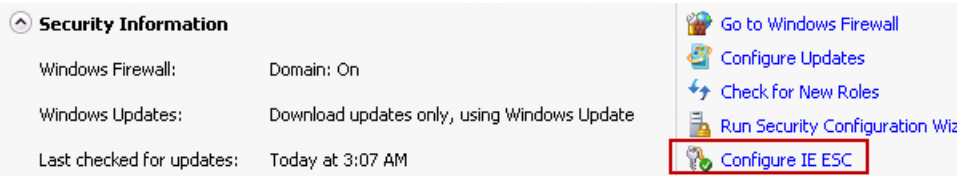


10. Click **OK**, and exit Internet Options.

Configuring NTLM via Group Policy

To create an NTLM transparent authentication policy using a Group Policy Object (GPO):

1. Log on to your Active Directory domain controller (DC) using a domain admin account.
2. Perform the steps listed in *Internet Explorer & Google Chrome* to enable NTLM in the Internet Explorer or Chrome browser on the DC.
3. To turn off Internet Explorer Enhanced Security Configuration:
   a. Open Server Manager.
   b. Scroll down to Security Information, and click **Configure IE ESC**.
   c. Turn ESC Off for administrators and users, and close the window.



4. Open Group Policy Management.
5. Right click your domain name (or the OU that contains the end users who will receive this policy), and click **Create a GPO in this domain, and link it here**.
6. Give your new policy a name, and click **OK**.
7. Right-click your newly-created policy, and select **Edit**.
8. Navigate to **User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings**.
9. Select **Import the current security zones and privacy settings**.

10. You may receive a warning about Enhanced Security Configuration. This is why the enhanced configuration was disabled in step 3, so that this policy will apply to workstations without enhanced security turned on. Click **Continue**.
11. Turn on Enhanced Security Configuration again, and repeat steps 4-9 to create a policy with ESC enabled. This ensures that workstations with either configuration are supported.
12. Close all open windows.

The changes will take time to replicate though your Active Directory, depending on your setup. This may be from 15 minutes to an hour; if you have a multi-site AD setup, it may take a day or two.

You can then set up a login script that will install the policy when end users log on to their workstations.

This method uses 2 files:

- login.bat
- ntlm.reg

The login.bat script contains two lines:

```
@echo off
regedit /s \\path\ntlm.reg
```

In the ntlm.reg script, replace <Box IP> with the IP address of your appliance:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Internet Settings\ZoneMap\Ranges\Range5]
"*"=dword:00000001
 ":Range"="<Box IP>"
```

Mozilla Firefox

Note

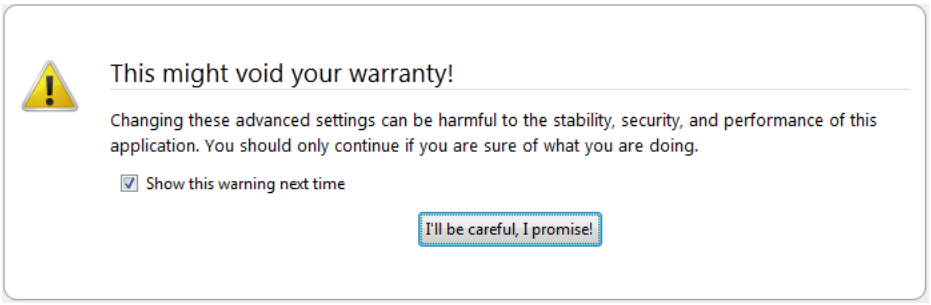
If you are configuring Firefox v38 or later on Linux, you must perform step 6 in the procedure below to ensure the browser falls back to NTLM v1. This is due to the Linux version having issues with NTLM v2 that can cause authentication failures.

The screenshots in this section are taken from Mozilla Firefox version 40.

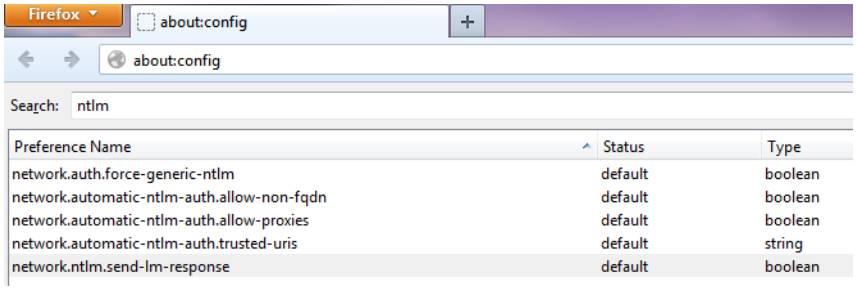
To enable NTLM transparent authentication in Firefox:

1. Open Firefox, and type **about:config** in the address bar.

2. Click **I'll be careful, I promise!** to open the advanced configuration page.



3. Type **ntlm** in the Search field.
4. Select **network.ntlm.send-lm-response** and double-click it to toggle it to on.



5. Double-click **network.automatic-ntlm-auth-trusted-uris**. In the box that appears, enter the IP address of the B1/B2 bridge interface on your appliance, and click **OK**.
6. If you are configuring Firefox on a Linux machine, double-click **network.auth.force-generic-ntlm-v1**.

   The Status is changed to **user set**, and the Value is changed to **true**.