WHITE PAPER: MALICIOUS ACTIVITY ASSESSMENTS WITH SWG

Confidence in a connected world. Symantec

Symantec Web Gateway v5

Performing Malicious Activity Assessments

For Symantec System Engineers and Partners

Symantec Web Gateway

Performing Malicious Activity Assessments

Table of Contents

Using Symantec Web Gateway to perform a Malicious Activity Assessment 3

The Rise of Malicious Traffic on Networks 4

Understanding the Phases in a Breach 6

Incursion 6

Discovery 8

Capture 9

Exfiltration 10

An Overview of Malicious Activity Assessments with Symantec Web Gateway 12

Setting up the Symantec Web Gateway for a Malicious Activity Assessment 13

Understanding the Results of a Malicious Activity Assessment 23

Monitoring for Malware and suspected Bot activity 24

How The Symantec Web Gateway detects Botnets 24

The Botnet Lifecycle 25

Investigating Bot Activity 27

Investigating a Potential Attack 30

Investigating the Top Sources of Infection 31

Additional Resources for Malicious Activity Assessments 32

Deploying the Web Gateway on an ESXi V4.x server 33

Using Symantec Web Gateway to perform a Malicious Activity Assessment

With the dramatic rise and increasing complexity of malicious traffic on networks today, it is vital for organizations to have visibility into potentially harmful activity in their environments. Employing traditional defensives, such as antivirus protection and email filtering, is as important as ever. However, the evolving threat landscape—characterized by Web 2.0 threats, botnets, command and control servers, and other types of malware—demands a proactive approach to uncovering threats and understanding the volume and impact of malicious activities, ones that often fly beneath the radar of typical safeguards. The first step is to assess current threat level of environment.

This document describes how to use the Symantec Web Gateway to perform a Malicious Activity Assessment of a customer environment. A Malicious Activity Assessment involves a simple deployment of the Symantec Web Gateway in a passive "Monitor Mode" configuration. Leveraging actual production data from the customer environment, this focused engagement quickly identifies the presence of installed and active malware, as well as other threats, on the network. The assessments are highly effective as they leverage new sources of security intelligence, the Symantec Global Intelligence Network, and DeepSight, which can also allow customers to gain early warnings to new and unknown threats.

Malicious Activity Assessments are not full deployments and as such require minimal tuning and leverage several default reports to illustrate the results. Ideal targets for Malicious Activity Assessments include customers running endpoint software with antivirus defences only, as well as customers who may have had a malware outbreak. The findings of typical Malicious Activity Assessments identify key areas for improved protection and response, resulting in discussions on the benefits of other Symantec products, such as those found in the Symantec Protection Suites.

This document provides:

- An overview of the trend and characteristics and malicious traffic and data breaches
- A guide to configuring the Symantec Web Gateway for these assessments
- A walkthrough of key reports to leverage for the results session with the customer
- A list of other helpful resources for deploying Malicious Activity Assessments

The Rise of Malicious Traffic on Networks

According to Symantec's most recent *Internet Security Threat Report*, Global networks faced more than 286 million cyber threats in 2010, as attackers employed more sophisticated methods that make malware harder to detect and more difficult to remove. Furthermore, the number of Web-based attacks increased 93% in 2010, and malware writers have been turning their attention to social-networking sites such as Twitter and Facebook, where it's estimated that 17% of links are connected to malware.

The threats are becoming more sophisticated and targeted. These types of attacks can be mounted anonymously and cheaply from anywhere in the world. Targeted attacks were very effective and had a higher success rate since they allowed hackers to break into enterprises and spy on employees in order to gather information that can be used to tailor social engineering methods that could trick the users. Targeted attacks against organizations are becoming harder to combat than earlier Internet-based attacks, which were much more widespread and indiscriminate. As an example, in recent years MasterCard disclosed a breach at Card System Solutions, a provider payment service for credit card companies. The incident exposed 40 million credit cards to criminals. The breach occurred by a malicious script placed on a computer that stored data at the facility.

When criminals launch such a targeted attack, they typically realize something of value and have a specific target in mind. Similar to bank robbers "casing the joint," attackers will employ various methods of research to gain knowledge of their target's environment. As such, criminals seek to understand the weaknesses of the environment before the attack. Often, the attackers use social engineering tricks—by way of spoofed emails and Web sites—to get users to unknowingly install malicious code that will show to the attacker vital information from inside the network. Good examples of these attacks are *whaling* and *phishing*. With whaling, cybercriminals leverage resources such as social networking websites to gain information about whom they want to target in an organization. These attacks focus on high-level, high-value individuals whose credentials, if stolen, can cause significant damage to their respective organizations. Once criminals get users to reveal IDs and passwords, they can then gain access to critical systems and information. In contrast to the more common Phishing attacks that deploy millions of emails in a scattershot approach, whaling usually involves a few thousand emails, often sent from a botnet with perhaps a few thousand compromised computers. Whaling attacks are harder to detect using conventional methods, as the attacks often use a company or contact that the person they are targeting trusts.

Symantec's report also identified a dangerous trend regarding malware. In years past, malware was delivered as self-replicating email viruses and network worms. The primary goal was rapid and widespread propagation, usually resulting in availability losses and extensive clean-up. According to report, Malware is now much more sophisticated and an essential part to nearly all large-scale data breach scenarios. Hacking gets the criminal in the door, but malware gets him the data. Naturally, the criminal will then want to lower the chance of detection in order to maximize the amount of data stolen. For this reason, malware becomes ever more directed, innovative, and stealthy. When an organization's network is compromised by malware, it is most likely using a rootkit to conceal its presence, making it difficult to detect and remove. By a wide margin, the most common malware delivery method was the scenario in which an attacker compromised a system and then installed malware on it remotely.

In another dangerous trend, cybercriminals have now started to use Web sites as vehicles to infect users. These Web sites are legitimate, popular sites that have been compromised to attack individuals that are browsing them. With malicious action against information systems and web servers, hacking is the leading cause of data loss. One supporting reason is that hacking is less subject to the constraints that limit other attack methods (for example, physical proximity, human interactions, special privileges). In addition, many tools are available to help automate and accelerate the attack process, which keeps the cost of attack fairly low for the criminal. According to Symantec, automated attack kits targeting Websites accounted for two-thirds of all Web-based attacks. The number of Web-based attacks grew 93 percent in 2010 from 2009. Those familiar with attack classification methodologies will know that the library of hacking and intrusion techniques is extensive.

An important corollary to the infection vector concerns the behaviour of malware once placed in the victim environment. Most malware captures and stores data locally, captures and sends data to a remote entity, or enables remote access to—or control of—the infected system. The most common of these were keyboard loggers or spyware. Usually these malware tools are used to capture authentication credentials, which are almost always sent to a remote attacker rather than stored locally for later retrieval. The small packet size for such data usually guarantees a better chance of undetected egress. Criminals often use these credentials for subsequent expanded attacks against corporate systems. In many large scale data breaches, malware that would capture and store data was found to be common among the breaches. These malware would also contain backdoor components that would allow the cybercriminal to gain access into the environment.

Newer, more elaborate varieties of malware utilities bypass data controls and encryption, creating vulnerable data stores that can later be retrieved from the victim environment. Examples of this new breed of malware include the usage of memory scrapers, sophisticated packet capture utilities, and malware that can identify and collect specific data sequences in unallocated disk space and from the pagefile. Traditionally, the term “stored data” has referred to non-transient items (e.g., in a log file or within a database on a hard drive, CD, or backup tape). Overlooked in this classification is the transient storage of information within a system’s RAM. Most application vendors do not encrypt data in memory and for years have considered RAM to be safe. The advent of malware capable of parsing a system’s RAM for sensitive information in real-time, has revealed this soft-spot in the data security armour.

Sophisticated malicious Internet-based attacks can go largely undetected by most antivirus software, especially software without Intrusion Prevention or advanced technologies such as Insight. Essentially, new malware threats are developed quicker than the antivirus companies can develop fixes. Today, the threat environment has transformed, as the players are more specialized and even more productive in terms of the malicious payloads they create. Often, attackers simply repack existing malware so its signature is undetectable by antivirus software scanners. Hackers also have increasing access to vulnerability data, which is discovered in applications in a more condensed timeframe, and shared in Hacker forums and sites. The exploits of these vulnerabilities can be developed almost as fast as the remediation patches.

Organizations often have a false sense of security that machines are protected while on the company network. Problems arise, however, when an executive, for example, takes his machine home or on a business trip in a less secured environment. During this period, the executive’s machine might be targeted with malicious code, which is then brought back into the company to do its task. Once off the company network, the machine is free to communicate back to its host to deliver the confidential corporate information it collected.

Understanding the Phases in a Breach

There are several loosely demarcated phases in a typical data breach. In this document, we refer to them as Incursion, Discovery, Capture, and Exfiltration.

Incursion

The incursion phase of a breach occurs where the criminals, hackers, organized crime groups—and even government entities in some cases—try to gain unauthorized access to data or a system. The criminals are aided by many tools that are readily available that automate and accelerate the incursion. Incursion into an organization’s infrastructure is often accomplished in a couple of ways:

- **SQL injection**—By analysing the URL syntax of targeted websites, hackers are able to embed instructions to upload malware that gives them remote access to the target servers.

- **Exploiting system vulnerabilities in another method**—In many cases, laptops, desktops, and servers do not have the latest security patches deployed, which creates a gap in the security posture. Gaps or system vulnerabilities can also be created by improper computer or security configurations. Cyber-criminals search for and exploit these weaknesses to gain access to the corporate network and confidential information.
- **Targeted malware**—Cybercriminals use spam, email, and instant message communications often disguised to come from known entities to direct users to websites that are compromised with malware. This section includes several different approaches that cybercriminals leverage to infect systems with malicious code.

Of these methods, malware has slowly risen to the top of most organizations' concern lists. A recent report estimates that there are around 600 million Windows-based computers infected with malware worldwide, and it estimates the cost of malware damage from $281 to $340 a machine. This works out to several billion dollars in lost revenue for companies worldwide. Such software can bring in Trojans and viruses, open backdoors, and report your users' browsing preferences to hostile and foreign sites. According to Wikipedia.org, "Malware (a portmanteau of "malicious software") is a software program designed to fulfill any purpose contrary to the interests of the person running it. Examples of malware include viruses and Trojan horses. Malware can be classified based on how it is executed, how it spreads, and what it does."

Over the past year, several companies appeared in headlines because of data leakage that was traced back to a compromised system that was infected with malware. These single incidents can cost companies millions of dollars in legal fees and investigation. These companies faced not only a loss of money and resources, but also a loss of customers and overall brand value.

Malicious tools enable attackers to gain access to a variety of valuable resources such as identities, credentials, hacked hosts, and other goods and services. On top of earning income from stealing data, attackers will also sell the tools of the trade. These tools usually will consist of botnets that can be used as part of denial of service attacks, to host phishing sites, relay spam, and as a launch pad for additional attacks. Spam and phishing products include spam software, spam relays, compromised computers to host phishing scams, and content such as phishing scam pages and phishing scam letters. Malicious code includes tools such as banking Trojans, back doors, and password stealers.

Bots, also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet. Often bots perform tasks that are simple and structurally repetitive, at a much higher rate than would be possible for a human alone. There are some cases where they are not used for malicious intent, but that is not common anymore. Today bots are used for a variety of different malicious uses cases:

- Spam
- Denial of service and distributed denial of service attacks
- Click fraud

- Keylogging
- Sniffing
- Phishing

Bots are good at hiding in the shadows of your computer so that they are not noticed. If you could easily detect that something was running on your computer, you would quickly remove or disable it. They often have file and process names that are similar, or even identical, to normal system file names and processes so that users won't think twice even if they do see them.

Discovery

After the initial incursion and cybercriminals get into the organization, the discovery phase starts. From the cybercriminal's perspective, the goal of this stage is to map out a corporate network, understand what information exists where, and how well protected that information is.
The criminals are depending on the infrastructure of companies not being appropriately hardened. Companies in many cases have not enforced strong IT policies around who should have access to what infrastructure and what information.

Cybercriminals also count on that fact that information is not being where people think it is. In many cases, well-meaning insiders, (well-meaning employees), take important information assets and move them to another location or system that may not be hardened appropriately. Many breaches happen by well-meaning insiders causing what we call data spillage. Cybercriminals can capitalize on this during the discovery phase since most companies do not know where sensitive information may have been inadvertently moved, copied, or relocated. The duration of the discovery phase depends on the cybercriminal’s skills, familiarity with the environment, the method of the attack, and the victim's defences. Data compromise can often occur minutes or hours after the discovery phase.

Activities performed during the discovery phase represent a direct threat. At this stage, the cybercriminal is accessing and assessing the value of the data. To the extent that the data being analysed is unencrypted, there is a significant risk of data loss. Whether it’s compromised intellectual property or sensitive customer data that is exposed for later use in identity theft, the discovery stage is where the potential losses become real.

Also, during the discovery phase, cybercriminals can exploit systems that have trust relationships with each other. Because business relationships with third-party business partners and vendors often require the exchange of confidential information such as 401(k) plans, outsourced payment processing, supply chain order management, and many other types of operational data, the scope of the threat gets exponentially worse during the discovery phase.

In this phase, attackers leverage port scanners to look for open ports and services, network mappers to determine with IP addresses are “live,” and vulnerability scanners to look for known weaknesses. The goal is to find information that can be used in the attack.
Hackers often use port scanning to identify all services or applications running on a machine. For example a port scan that finds port 80 as open indicates that a Web server is running on that system. The cybercriminal can use this information to launch an attack against based on a vulnerable service running on it, or identify a system based on a service (1433 SQL) that the system might contain data of interest. Intrusion Detection Systems (IDS) or Security Information Management (SIM) type products can be used to identify hackers performing these types of scanning in an environment. From an external perspective most of these types of scanning can be blocked by a firewall. If a hacker has already compromised an internal system, and is using the system to perform the scanning, then a firewall might be useless unless it is a host-based firewall.

In the discovery phase the cybercriminal might also use keyboard loggers and sniffers to collect data to help map out the environment. Network traffic data can contain vital information to help map out a network, but can also contain data like credit card or personal data if not encrypted. Once the cybercriminal has a foothold they can determine the value of the data and whether the data is worth stealing.

Capture

In the Capture stage, which occurs after the criminals have penetrated the organization and surveyed the data and assets, the criminals narrow down the most valuable information assets that are the least well protected. As the name implies, this is the phase where the criminal steals or takes controls of the asset. However, they don’t extract the information yet—that occurs during the final exfiltration stage. This objective here is similar to deciding whether to crack a safe: will the reward be worth the effort?

Given the risk and effort involved in breaking into systems, cybercriminals look for data with high value. At the capture stage, criminals perform the trade off or cost-benefit analysis, based on the prevailing value of the assets versus how well protected the data is. For example, bank account numbers, credit card records, social security numbers, passport numbers all have specific values in criminal markets. In performing the trade off, the criminals may decide that it’s more profitable to target employee desktops as opposed to the corporate servers. Similarly, they may not target the official customer database, since it would be carefully guarded. However, they may choose to target a development copy of the same database, or an end user workstation that has valuable information, or a file server with open permissions.

As the cybercrime market evolves, attackers, targets, and techniques do as well. The value associated with selling stolen credit card data has dropped over the past few years. The big profits now reside in stealing personal identification number (PIN) information together with associated credit and debit accounts. The higher value commanded by PIN data has spawned a cycle of innovation in attack methodologies. The value associated with selling stolen credit card data have dropped from between $10 and $16 a record in mid-2007 to less than $0.50 a record today. Identity data still remains a high selling commodity on the black market. Cybercrime has become a bigger market the drug trading industry.

Exfiltration

The cybercriminal's purpose in the exfiltration stage, which is the final stage in a data breach, is to get the captured data out of the company to a safe location. The cybercriminal will take many precautions when extracting data out of the targeted organization. For example, he will often extract the stolen data to another system other than his own, but one that he can access at his leisure. As a further safeguard, he might divert the data to different legal jurisdiction. He might also encrypt the data during the transfer process.

A key enabling tool for exfiltration is bot technology. These programs can be configured to connect back to a given bot master or bot herder. Bots are normally initially infected by browser exploits, Trojans or viruses. Once the machine has been compromised, it will await instructions from the botnet master. From here, the bot master can transfer software down to the compromised machine that could then be used to steal data on the network or the user's credentials.

Today the most common method for communication between bots is over HTTP, which uses HTTP requests to inject commands, as opposed to the normal persistent connection of IRC, which was previously the most common method of communication used by bots. Using HTTP communication will make these bots harder to find. If you know, for example, what the requests look like, you can sniff for them, or you can use proxy logs. One of the challenges that this provides, compared to an IRC-based botnet, is that Web traffic (along with peer-to-peer traffic) to the outside world is the bulk of the backbone traffic that we see. Consequently, you have to sift through an enormous volume of data to identify the malicious traffic. IRC traffic is easier to block, using a rule on an IPS that watches for IRC traffic. But with HTTP botnets, you can't just block the Web traffic as TCP port 80 will for the most part be normal activity through the network. When the bot wakes up, it connects to a website that has a package waiting for it, and then the package is delivered. From the perspective of a cybercriminal, this is a much more stealthy method of exfiltrating data then with the use of IRC or P2P alone.

A closer look at a bot: Zbot (or Zeus)

- Installs itself as at the system level and spawns at startup time
- Opens backdoor for remote user
- Steals online credentials
- Uses HTML injection technique to get credential information
- Uses HTTP for communication to the command and control server
- When the bot connects to command and control server, it will download its instructions to execute

Cybercriminals, and malware, commonly use the file transfer protocol, or FTP, for exfiltration. FTP is a network protocol that enables the transferring files between computers. The protocol allows user-based authentication and anonymous authentication. It also supports command line operations, which make it easy to automate and batch tasks. Cybercriminals will often use FTP to upload stolen data to a FTP drop server. FTP is attractive for cybercriminals because it is a communication method that is allowed out in many organizations. It is also enabled by default in some operating system installations.

Here's how a typical FTP-based exfiltration works, using the "metafisher" bot as an example. First, the malware installs itself as a Browser Helper Object in Internet Explorer. Essentially it configures itself as an add-on. Once working behind the scenes as an add-on, it operates as a "man in the middle," stealing data on the computer or capturing login information entered into banking websites. Once collected and captured, the stolen data are sent via FTP to an FTP drop server, selected based on user location. In the final retrieval stage to finish the exfiltration, the cybercriminal accesses the data on the FTP drop server based on the country the data stream came from and by a unique identifier of the infected user's machine.

As mentioned previously, P2P technology is also a favoured communication method for the cybercriminal. P2P technology refers to a distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances. P2P gained popularity with services for music and file sharing, with Napster, Bit Torrent, eDonkey being just a few of the well-known networks. The advantages of P2P didn't go unnoticed among malware writers and cybercriminals. P2P soon became a new way to issue commands to malware and capture and exfiltrate data. From a

Cybercriminal's perspective, P2P offers significant benefits, notably an efficient way to manage malware and criminal activities without a single point of failure, which would be the case with other networks when the centralized database or server went down or was taken offline.
P2P offers a high level of anonymity. It's next to impossible to identify an attacker in a P2P network.
For these reasons, P2P networks also lend themselves as prime vehicles for exfiltration.

An Overview of Malicious Activity Assessments with Symantec Web Gateway

Reacting to and remediating a malware outbreak can be a costly and time consuming exercise. With the Malicious Activity Assessment, you can help customers proactively identify security weaknesses and understand the key ways to strengthen defences to reduce the risk of malware exploitation. The assessment leverages a proven process to audit and analyse a customer's environment to identify weaknesses. With powerful reporting and detection tools, you will be able to provide timely recommendations and guidance for the customer.

Malicious Activity Assessments with the Web Gateway	
Key Goals	• Identify presence of installed and active malware on network • Target customers with ineffective endpoint protection
Overview	• 7 to 15 day deployment to assess threat level of environment • Analyses/discovers threats on traffic from production environment • Monitors for malicious traffic, malware/suspected bot activity & endpoint threat activity • Draws on intelligence from Symantec Global Intelligence Network and DeepSight
Customer Benefits	• Understand the volume and impact of malicious activities • Achieve early warnings to unknown threats • Identify key areas for improved protection and response • Leverage new sources of security intelligence

Setup/Configuration Summary	Customer Requirements
• Deploys in Monitor Mode (not complete Installation or POC) • Requires Span or Tap configuration • No impact on other equipment or software	• Complete of pre-engagement Technical Questionnaire • Ability to configure network for SWG placement • Executive commitment for assessment process/outcome • IT Staff to participate in process (approx. one day) • Key stakeholder participation in presentation of results

Setting up the Symantec Web Gateway for a Malicious Activity Assessment

You can install the Symantec Web Gateway inline or off a tap or span port on a switch. For Malicious Activity Assessments, Symantec recommends that you install off a network tap or span port. For the Malicious Activity Assessment, the Symantec Web Gateway will *monitor* network activity *but not block* malicious traffic. You will need to fully configure the Symantec Web Gateway before the monitoring of network traffic begins to take place.

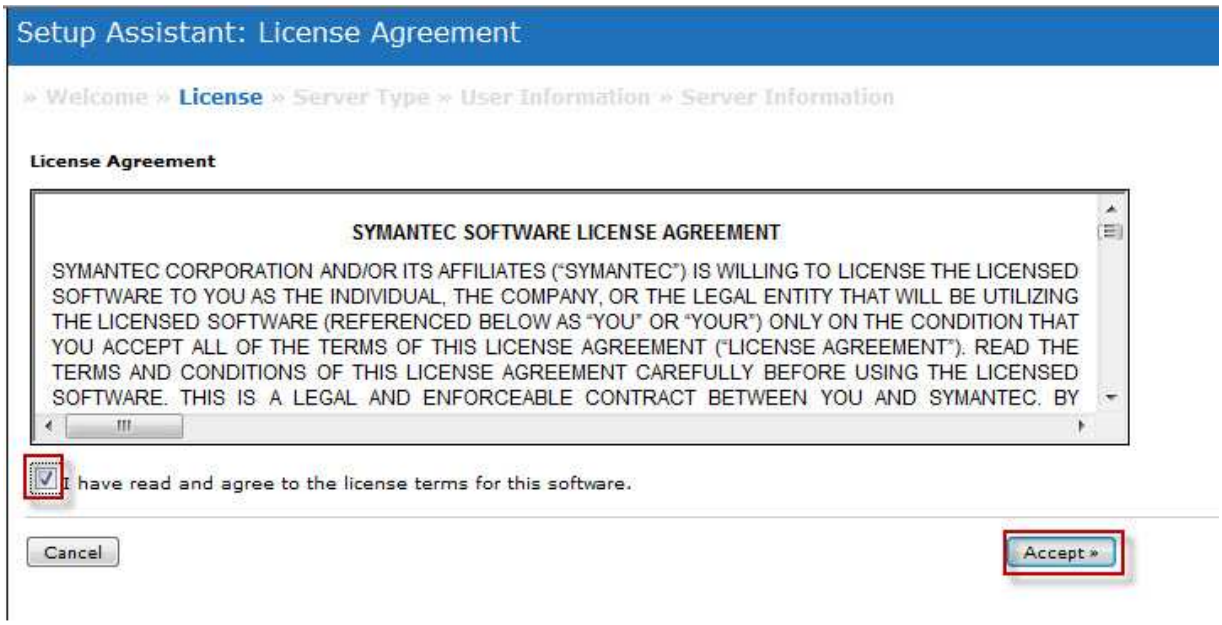
To deploy the Symantec Web Gateway, you will need to several pieces of information from the customer – these are detailed in a pre-engagement Technical Questionnaire that you can access <here> to send to the customer for completion. Some of the information required follows:

- Obtain a list of the internal networks the Symantec Web Gateway will be protecting (the subnet and net mask for these networks will be required).
- Obtain the IP addresses of any mail and proxy servers that exist in the networks that will be protected by the Symantec Web Gateway
- Identify an IP address, net mask, gateway, and DNS server to assign to the Management Interface on the Symantec Web Gateway
- Obtain a 30-day temporary license file. For instructions on how to receive the file by email, visit the following location: **https://www4. symantec. com/Vrt/offer?a_id=85595**
- Identify the IP address of an SMTP server that Web Gateway can use to send email alerts
- Identify the IP addresses of any IDS, IPS or any critical systems that you want the Symantec Web Gateway to ignore on the internal network, or on the Internet.
- Provide access to certain ports and sites. These are documented in the Symantec Web Gateway Implementation Guide. You can find the latest product documentation at: **http://www. symantec. com/business/support/documentation. jsp?language=english&view=manuals&pid=58161**

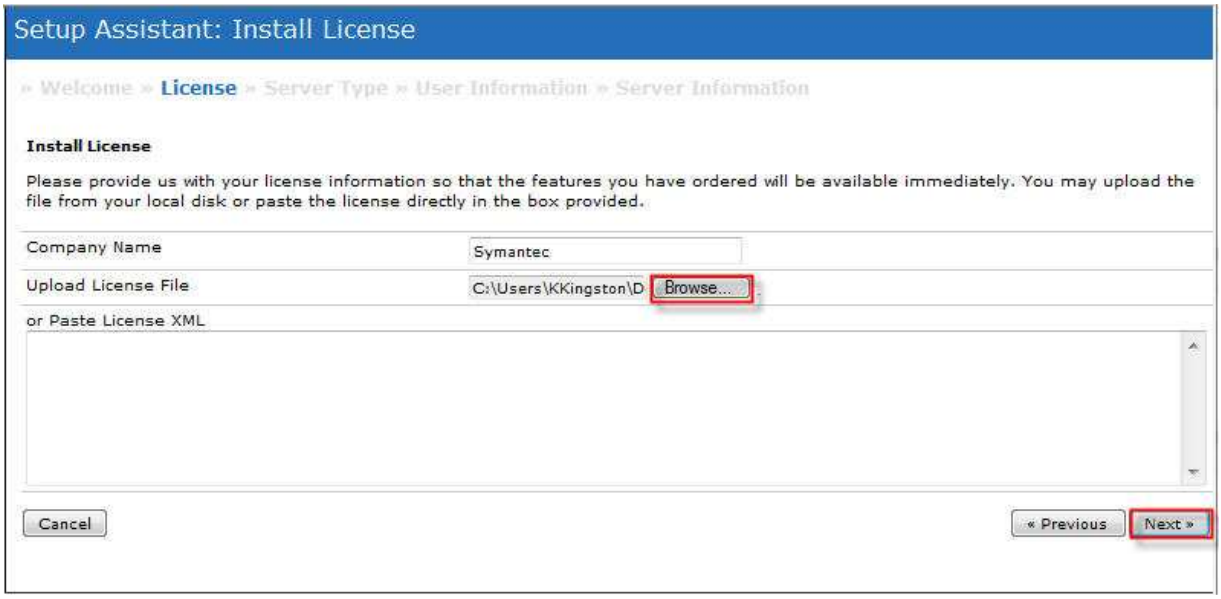
To complete the Setup Assistant for the Symantec Web Gateway:

1. Before racking the appliance, power on the Symantec Web Gateway, connect a crossover cable from a laptop or desktop, and then connect to the Symantec Web Gateway.
2. Set the IP address of the laptop to 192. 168. 254. 253 with a netmask of 255. 255. 255. 0.
3. Using a supported Web browser, connect to the Symantec Web Gateway on **https://192. 168. 254. 254**. When the following page appears, click the **Next** to continue

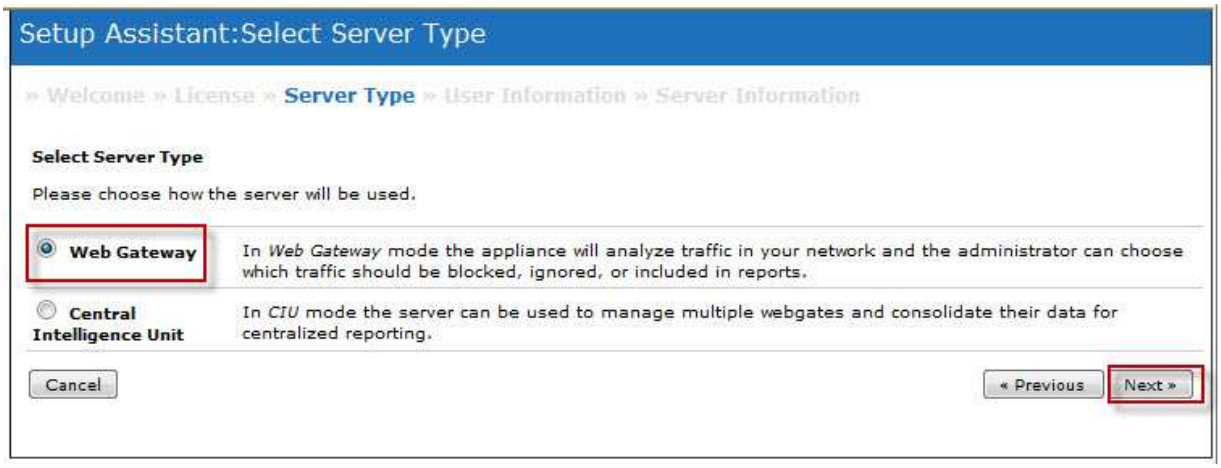
4. On the next page check the box to agree to the license terms and click **Accept**.



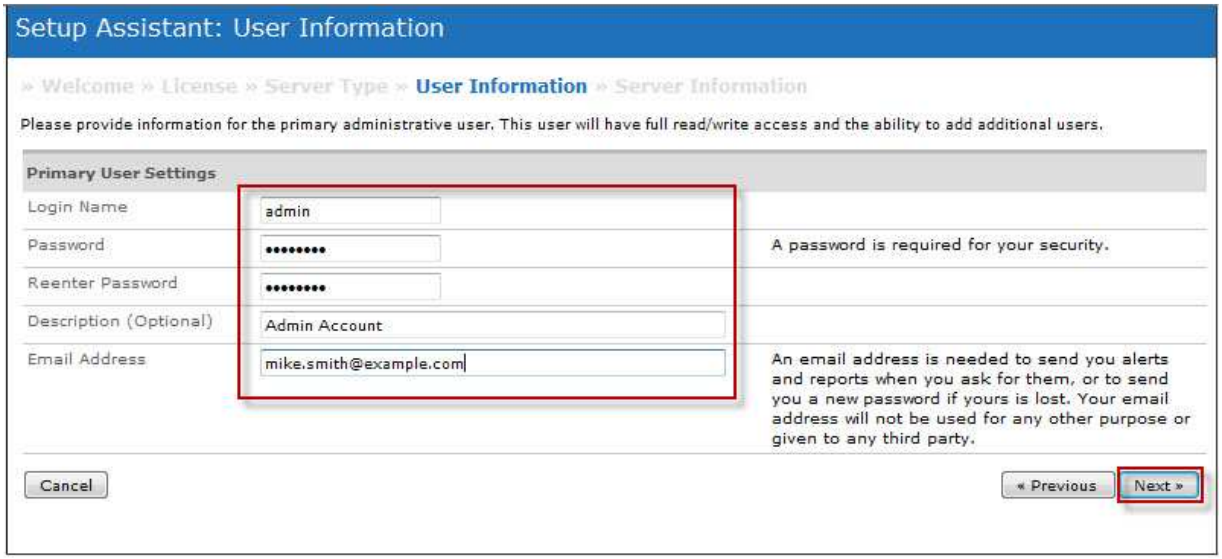
5. On the Install License page, complete the **Company Name** field, then browse to select the temporary license file obtained earlier. Note if in file is still in ZIP format, you need to extract the file to an SLF before you can add the license. Click **Next** to continue.



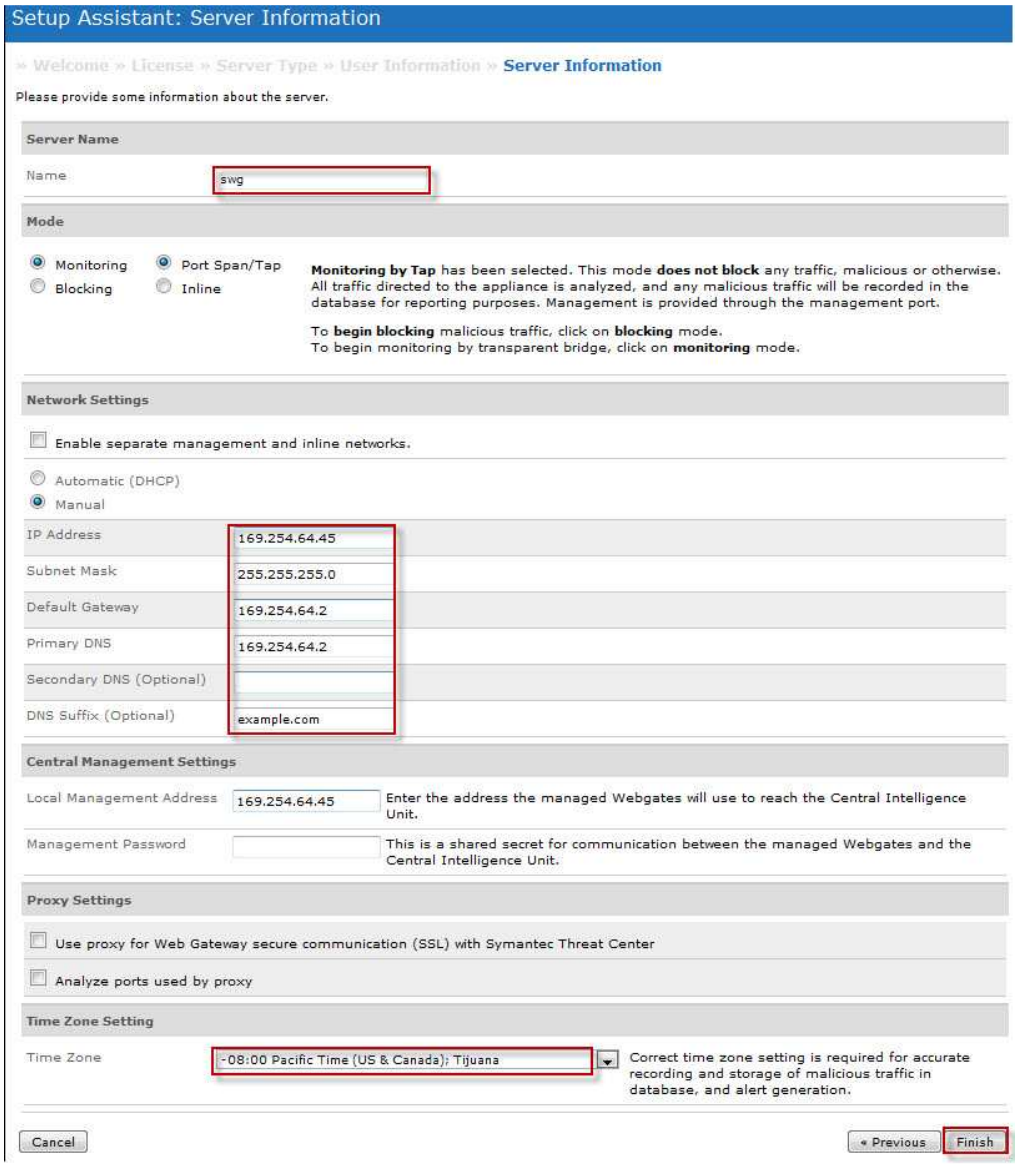
6. On the Select Server Type page, select Web Gateway and click **Next**.



7. On the user information page, complete the **Login Name**, **Password**, and **Email Address** fields for the main administrative account you will use to manage the Symantec Web Gateway Web interface. Click **Next**.



8. On the Server Information page:
   a. Complete the **Name** field the Symantec Web Gateway. This will be the hostname for the Web Gateway.
   b. Under Mode, select **Monitoring** and **Port Span/Tap**.
   c. Under Network Settings, enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **DNS Suffix** for the Symantec Web Gateway. This is the domain part of the A record that has been created for the Symantec Web Gateway in DNS.
   d. Under Time Zone Setting, select the appropriate Time Zone.



Important Note when deploying with proxies: If the Symantec Web Gateway needs to go through the proxy to connect to the Symantec backend to get definitions, database and software updates, enable the **Use proxy for Web Gateway secure communication (SSL) with Symantec Threat Center** option (under Proxy Settings). Enter the IP address of the proxy server and Proxy Port the Symantec Web Gateway should use. The Symantec Web Gateway must have unauthenticated access through the proxy to get these updates, so the proxy may need to be configured to allow this.

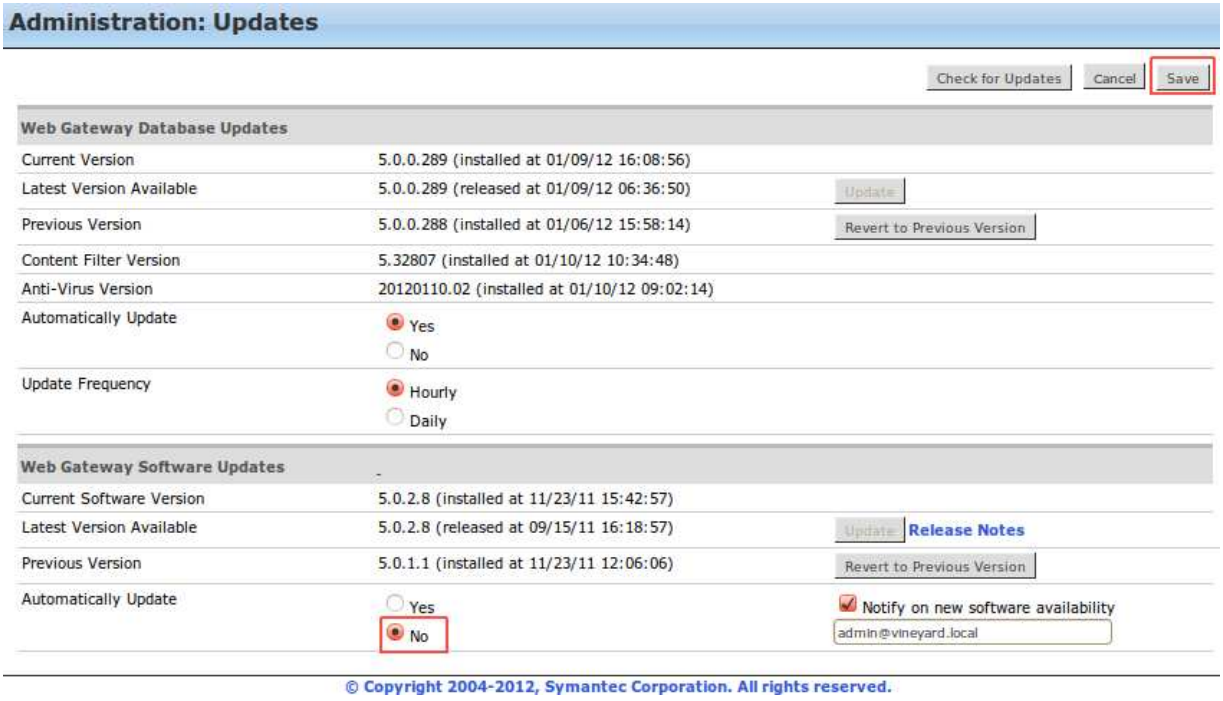
The Symantec Web Gateway also needs to know which ports are being proxied in the environment as it monitors web traffic. Select **Analyze ports used by proxy**, enter the value(s) for the **HTTP Proxy Port/Port Range** and also enter a value for the **FTP Port**.

9. Click the **Finish** button to complete the Setup Assistant.

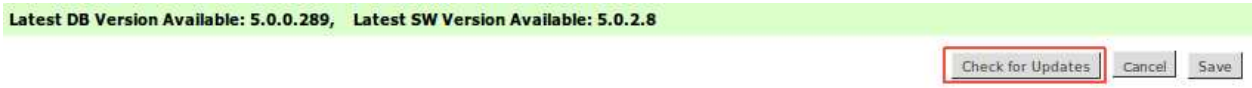
   At this stage, the browser loses its connection to the Symantec Web Gateway and the Symantec Web Gateway takes on its newly assigned IP address. You will next need to cable the appliance to the switch and then connect to the new IP address to make the additional configuration changes described below.

To complete the final configuration phase for the Symantec Web Gateway:

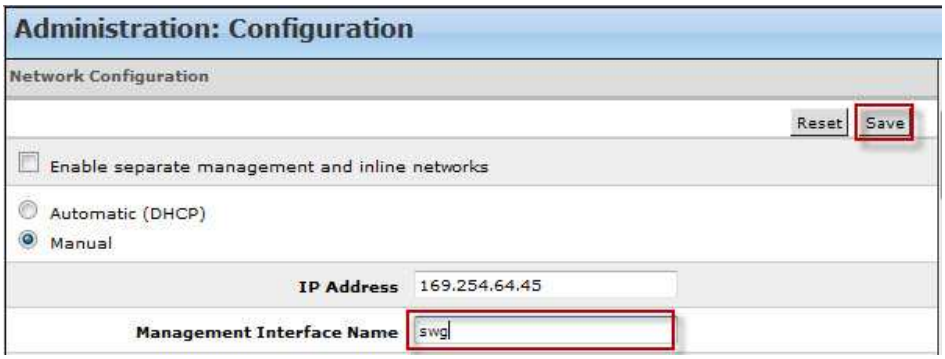
1. Remove the crossover cable from the Symantec Web Gateway and the computer you used for configuration.
2. Rack the Symantec Web Gateway and cable the Management Interface to the core switch in the network using a standard patch cable.
3. Using a computer on the network, connect to the Symantec Web Gateway via HTTPS to the new IP address. If you are using the laptop/computer used originally to configure the Symantec Web Gateway, ensure that you cable and reconfigure machine so that it is back on the network. Login using the username and account that were created during the Setup Assistant.
4. Once logged into the Symantec Web Gateway, go to the Administration -> Updates page. Under Web Gateway Software Updates, change the **Automatically Update** setting to **No** then click **Save**.



5. When the page refreshes, click **Check for Updates**. Apply any Web Gateway Database Updates or Web Gateway Software Updates by clicking the **Update** button under each section of the page (the 'Update' buttons can only be clicked if new updates are available, only one update can be done at a time). Software Updates will take longer and will sometimes reboot the appliance once completed.



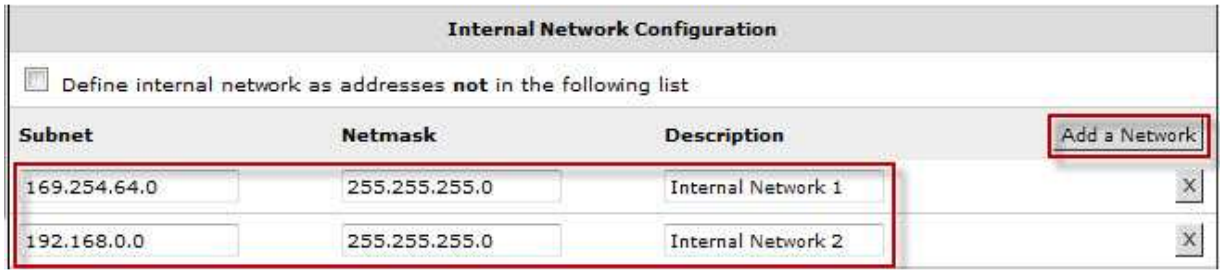
6. Once any updates have been applied, go to the Administration -> Configuration -> Network page. Under Network Configuration, set the **Management Interface Name** to be the same name you gave the appliance during the Setup Wizard. Click **Save**.



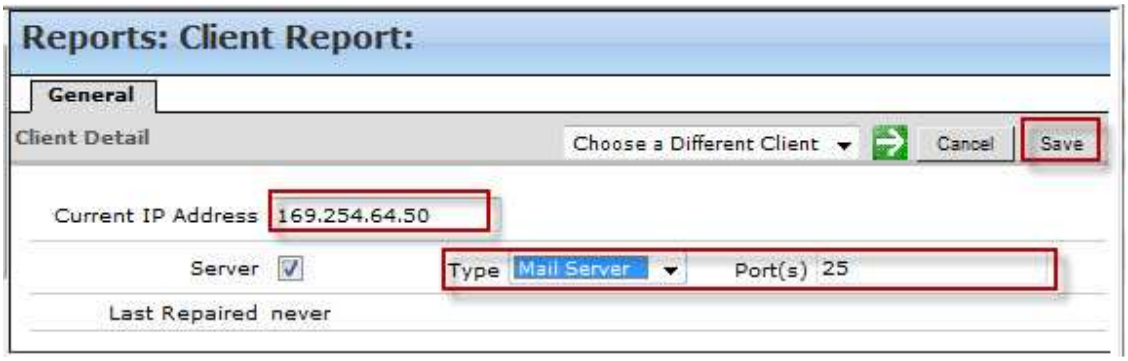
7. Under Internal Network Configuration, click **Add a Network** to define all of the internal networks the Symantec Web Gateway will be protecting in the environment. You need to specify the Subnet and Netmask for these networks. For tracking purposes, add the optional Description of these networks for tracking purposes. Once you have defined all the internal networks, click **Save** in the top right hand corner of the page.

   When the following points are **both** true:
   a. You are deploying in an environment with a proxy
   b. All network traffic inspected by the Symantec Web Gateway is destined to proxy destination addresses. This situation usually occurs when the Symantec Web Gateway is installed in front of a proxy

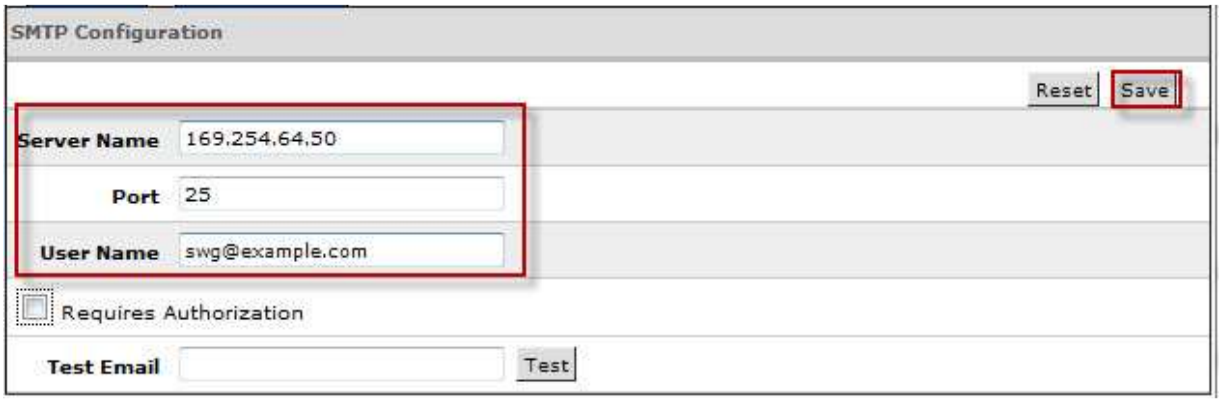
   You do not need to define all the internal networks. You can enable the **Define internal network as addresses not in the following list** checkbox and then enter the proxy addresses that are being targeted by the client traffic as the internal network(s). Consequently, the Symantec Web Gateway will compute any address that is not the proxy addresses as internal.



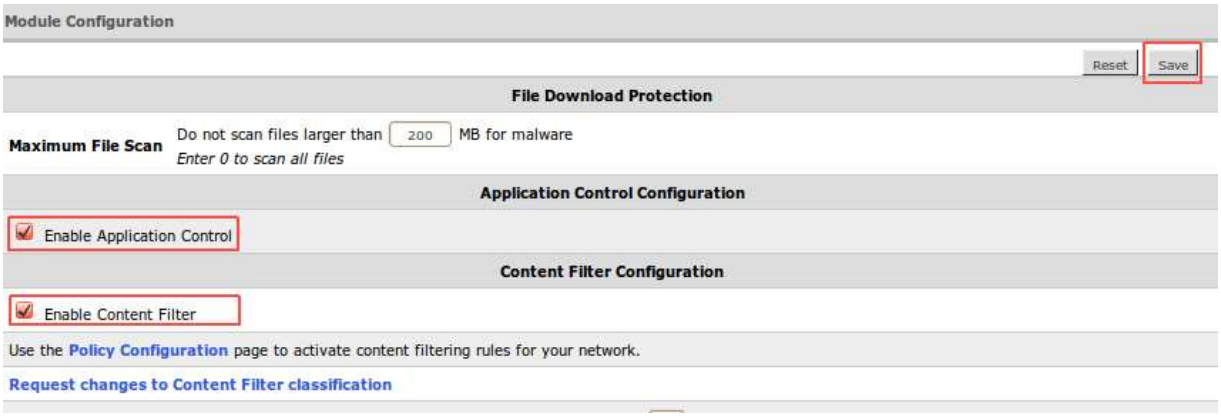
8. The Symantec Web Gateway needs to be aware of any mail or proxy servers that also exist in the network. Go to the Administration-> Configuration-> Servers page to add the servers individually. Click **Add a Server**, enter the IP address of each server beside **Current IP Address** and from the dropdown choose whether it is a Mail or Proxy server and adjust the port if different from the default. Click **Save** and repeat for the rest of the servers in the environment.



9. Go to the Administration-> Configuration-> Email page. In the **Server Name** field, enter the IP address of the SMTP server that the Symantec Web Gateway should send alerts to. Leave the **Port** settings as the default, unless SMTP is listening on a non-standard port. In the **User Name** field, enter a relevant SMTP address from which alerts will be sent in the environment (for example, web_gateway@example.com. Normally, the **Requires Authorization** checkbox can be unchecked. Click **Save**.

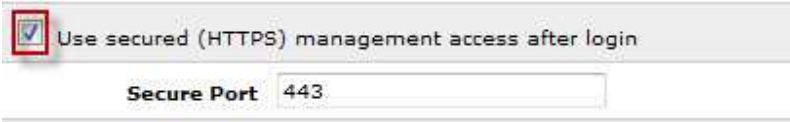


10. On the Administration-> Configuration-> Modules page, check the **Enable Application Control** field and **Enable Content Filter** field and then click **Save**.

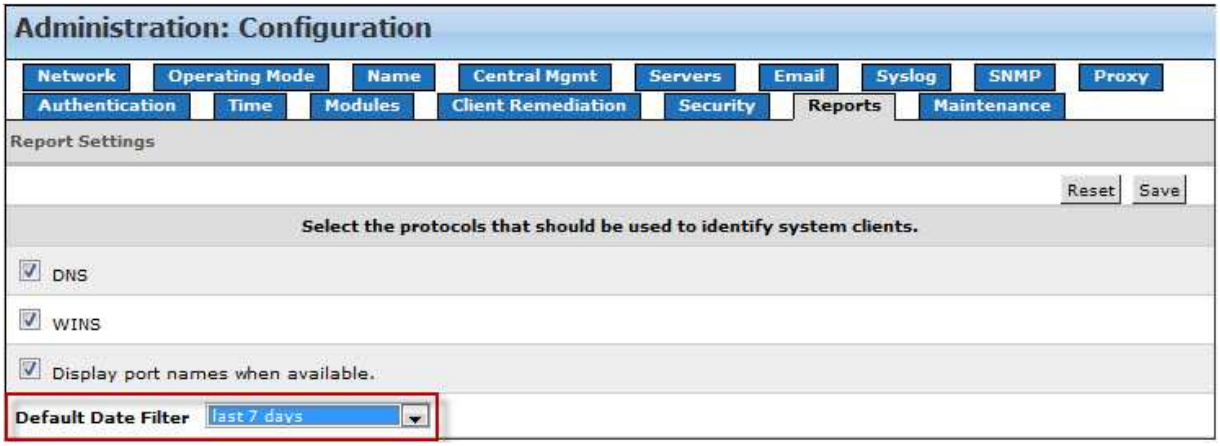


11. On the Administration-> Configuration-> Insight page, check the **Enable Insight Policies** field, and then click **Save**.

12. On the Administration-> Configuration-> Security page, check the **Use secured (HTTPS) management access after login** checkbox, and then click **Save**.



13. On the Administration-> Configuration-> Reports page, set the **Default Date Filter** drop down to **last 7 days**, and then click **Save**.



14. On the Administration-> Configuration-> Maintenance page, in the 'Incident History' section, set the **Keep incident history for** setting to **30** days and then click **Change**.

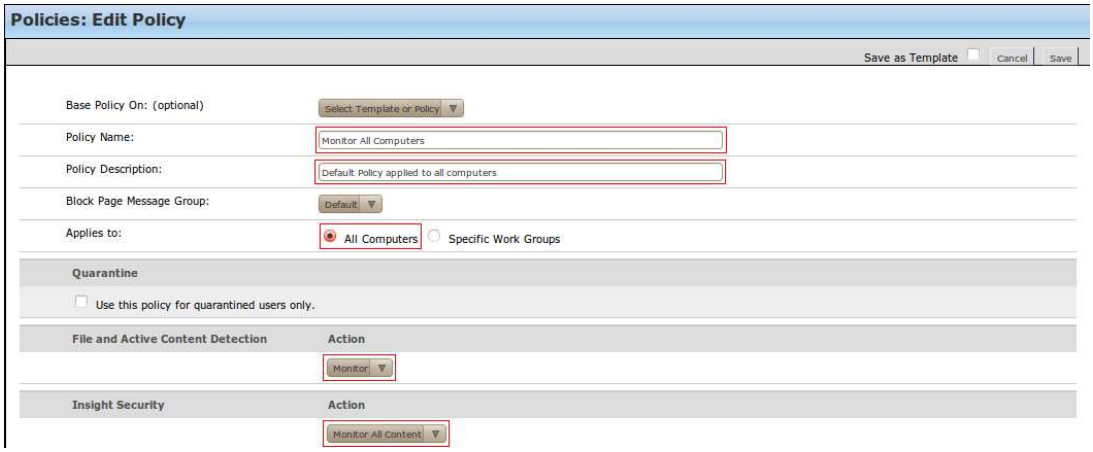
15. If a customer has any IPS or IDS devices on the network, or if they want the Symantec Web Gateway to ignore traffic from any critical systems on the internal network, or external networks on the Internet, these devices should be added to the Whitelist on the Symantec Web Gateway.

    To add systems to the Whitelist, go to the Policies -> Whitelist page. Click the button to 'Add a Whitelist Entry'. Add the IP address to be Whitelisted (it's probably a good idea to also add

a comment for reference). Click **Save**. Repeat the process for any other IP addresses to be added.

We are now ready to configure the policy to apply in the network.

16. On the Policies-> Configuration page, click **Create a New Policy** and then enter a **Policy Name** and **Description**. In the **Applies to** section, select **All Computers**. Set **File and Active Content Detection** and **Insight Security** to **Monitor.**



17. Leave the **Spyware Default** setting at **Monitor**. This configuration allows the Symantec Web Gateway to monitor the downloading of malware threats, monitor users accessing known malware sites, identify malware and botnet infected machines on the network and report on any potential attacks happening over the network.
Under **Application Control** select **Monitor All**.

18. Scroll down to **Content Filter** and select **Monitor All**. If a more granular monitoring is required, ensure that the **Malware** and **Spam** categories are selected for monitoring. Click **Save** in the bottom right hand corner of the page.

19. After saving the policy, click on **Save an Activate Changes** on the top right corner.

At this stage, you can place the Symantec Web Gateway into production. As stated previously, you can either use a network tap or a span port on the switch.

- **Using a network tap**—If using a network tap, you will need to disconnect the main network connection momentarily while the tap is placed in the network. Symantec recommends that you perform this action outside of working hours. To put the Symantec Web Gateway into production, disconnect the main internet link from the core router or firewall to the core switch in the network. Then plug the cable into the network tap provided. Next, plug the cable from the network tap back into the core switch in the network. Next, plug a second cable from the network tap into the Monitor interface on the Symantec Web Gateway. At this stage the Symantec Web Gateway should be monitoring network traffic.

> **Note:** If deploying using a network tap in an environment with a proxy, place the network tap between the proxy(s) and the core switch rather than the core router/firewall and the core switch in the network as mentioned above.

> **Note:** Symantec does NOT provide the TAP device. If the customer would like to deploy the MAA by using a network TAP, they would need to provide the TAP.

- **Using a span port on a switch**—Configure the source port for the span to the port that connects the core switch in the network to the gateway or firewall. Configure the port to transmit both received (Rx) and transmitted (Tx) traffic. Cable the destination span port from the switch to the Monitor interface on the Symantec Web Gateway. At this stage the Symantec Web Gateway should be monitoring network traffic.
-

> **Note:** If deploying using a span port in an environment with a proxy, the source port of the span should be configured to be the port that connects the core switch to the proxy(s) rather than the gateway or firewall as mentioned above.

Understanding the Results of a Malicious Activity Assessment

Before going over the results of an assessment, it is helpful to understand how The Symantec Web Gateway detects malicious traffic. The appliance employs several different methods, such as:

- Internet destination scanning using the Global Intelligence Network and Deepsight IP/URL watch lists
- File scanning using antivirus engines and heuristics
- Malware phone-home detection using network signatures
- Bot detection using network signatures and behavioral analysis

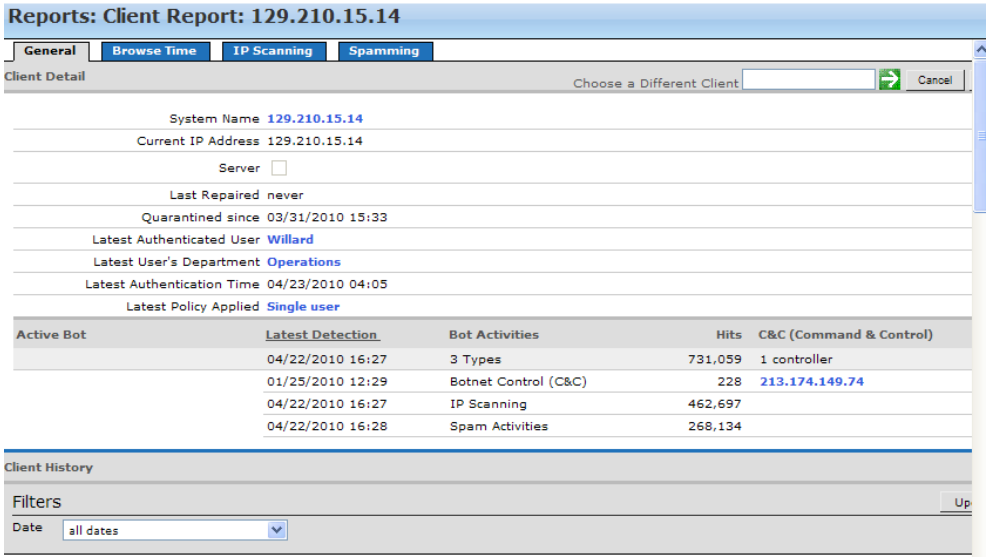
The Symantec Web Gateway can inspect traffic and downloads for malware and bot behavior. As The Symantec Web Gateway monitors connections to Web sites, it compares the IP/URLs to a watch list maintained by Deepsight to determine if the IP/URL is identified as malicious. The Symantec Web Gateway will also inspect communication to and from the internal network to the Internet looking for the behavior of command and control sessions, other phone homes or the transmission of malicious files. Using signatures The Symantec Web Gateway can identify malware and monitor systems that are trying to send spam or perform transfers or scans.

When The Symantec Web Gateway detects malware and Bot behavior, it classifies the traffic in several different ways:

1. **Suspicious**—Activity identified that is a low risk.
    a. Communication to a malicious IP but no other high risk activity detected
    b. System performing a port scan but no other activity

2. **Active**—More than one Bot behavior has been identified, and at least one of the behaviors is a higher risk
    a. Communication to a malicious IP followed by sending SPAM
    b. Communication to a malicious IP followed by a malicious file download
    c. IDS/IPS signature detected a specific malware

3. **Inactive**—System has not shown behavior for more than a week



4. **Potential Attack**—An attack was targeted at an internal system, but the system did not respond. This situation could occur when the system being targeted is not listening on the port that the attack is targeting or the system is patched for the vulnerability.

Reports: Potential Attacks: Spyware

Spyware | IP Scanning | Spamming

Filters — Add Filt

Date: all dates

AND: Select Filter Data | Select Filter Condition

Results 16 Potential Attacks — Report

Filter Dates 04/21/2010 - 04/23/2010
Report Run Fri Apr 23, 2010 4:32:13 PM PDT

Show 30 per pa

With Selected Items... — 1 - 16 of 16 | «« First | « Previous | Next » | La

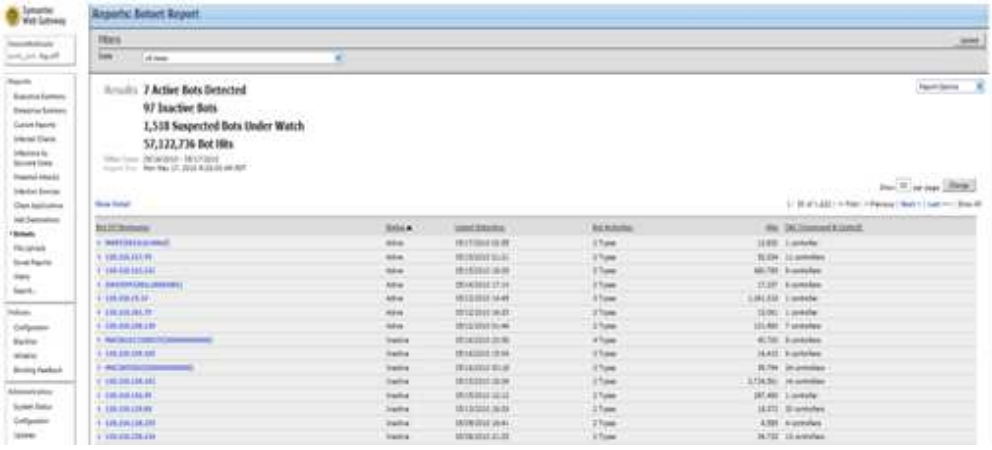
[all]	Latest Detection	Target	Target Port	Attacker	Attacker Location	Malware Name	Severity	Category	Action
	04/23/2010 04:09	129.210.238.134	4744	77.68.42.111	Gloucester, U.K.	Botnet C&C	Major	Botnet	Monit
	04/23/2010 03:47	adiemus.org	49402	208.100.20.83	Chicago, IL, U.S.A.	Botnet C&C	Major	Botnet	Monit
	04/23/2010 00:22	SCUUC17 (001e4fa87c5f)	3909: surfcontrolcpa	208.77.165.168	Sunnyvale, CA, U.S.A.	sharK	Critical	Trojan	Monit
	04/22/2010 22:25	129.210.216.124	64130	24.6.122.120	Los Gatos, CA, U.S.A.	sharK	Critical	Trojan	Monit
	04/22/2010 21:09	129.210.239.64	55427	63.80.4.111	San Jose, CA, U.S.A.	YKW	Critical	RAT	Monit
	04/22/2010 20:12	adiemus.org	54800	216.18.228.174	Seattle, WA, U.S.A.	Botnet C&C	Major	Botnet	Monit
	04/22/2010 19:16	129.210.146.72	51903	63.80.4.95	San Jose, CA, U.S.A.	sharK	Critical	Trojan	Monit

5. **Infected Client Detection**—When a system gets infected with malware, it will normally try to transmit some kind of 'call home' segment in a particular pattern back to the Internet. The Symantec Web Gateway uses network fingerprints based on these patterns to detect and block these Infected Clients on the network.

Reports: Client Report: 129.210.218.246

[all]	Latest Detection	Login Name	Detection Name	Category	Severity	Action	Detection Type
	07/15/2010 16:15	Phiala	WeatherBug	Potentially Unwanted Software	Minor	Monitored	Infection
	07/15/2010 16:01	Phiala	AlOt Toolbar	Browser Hijacker	Major	Monitored	Infection

Monitoring for Malware and suspected Bot activity



How The Symantec Web Gateway detects Botnets

The Symantec Web Gateway inspects inbound and outbound network traffic and queries the Deepsight list to determine if the traffic contains IP addresses associated with Bots. The Symantec Web Gateway also detects patterns of typical Bot traffic such as:

- Command and control communications
- IP scanning
- Spamming

Behaviors are examined to determine if the Bot is active. Single patterns are considered “Suspect,” as they may include false positives. Dormant Bots are marked “inactive.”

The Botnet Lifecycle

Phase 1: Initial Infection

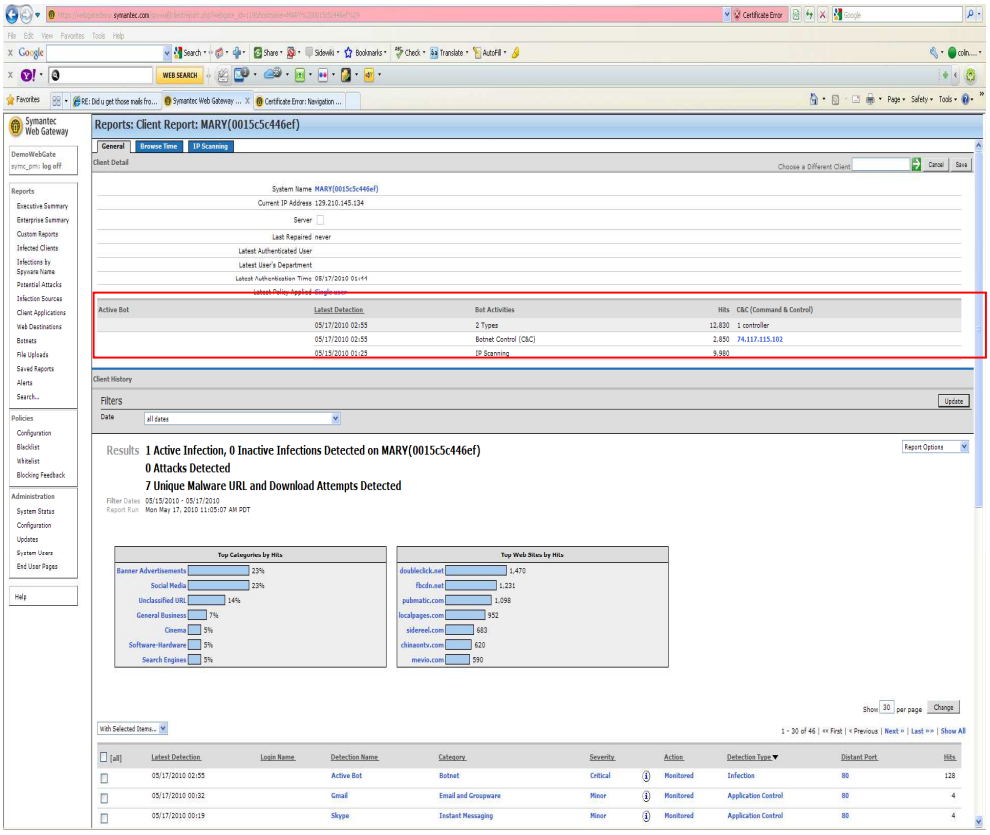
- Trojan Download
- Social engineering
- Can come through multiple sources
- Compromised Websites
- Questionable file downloads
- Instant message file downloads
- Email attachments
- P2P file downloads

In this phase, The Symantec Web Gateway employs several components to detect the initial infection. The Symantec Web Gateway scans file downloads occurring on HTTP, FTP and IM for malicious content. ActiveX and other client browser executable content is scanned as well looking for malicious content. The Symantec Web Gateway also monitors attempts to access IP addresses that are known to be bad.

Phase 2: Bot Activites and expansion

- Bot scans networks
- Bot reports back to command and control
- IP scans
- Spamming
- File transfers
- Can be in many forms (IRC, HTTP, SMTP, etc.)

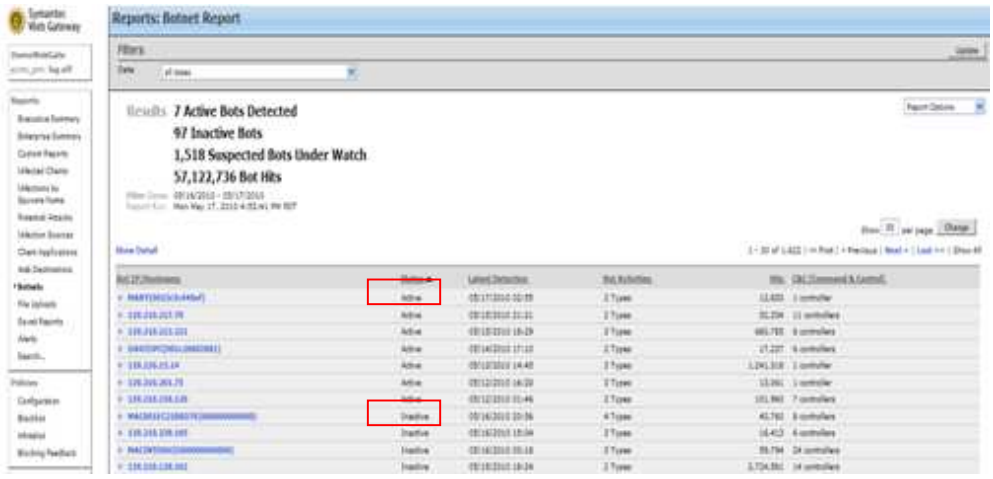
In this phase, the Symantec Web Gateway uses behavioral analysis for correlation with other bot activities to increase accuracy and minimize false positives. A bot is marked as “Suspect” and then “Active” as the behavioral detection progress. The Symantec Web Gateway uses behavioral fingerprints to look for known Bot behavior. The following example depicts a Bot that is marked as active based two behaviors detected.



Phase 3: Bot goes dormant until next command

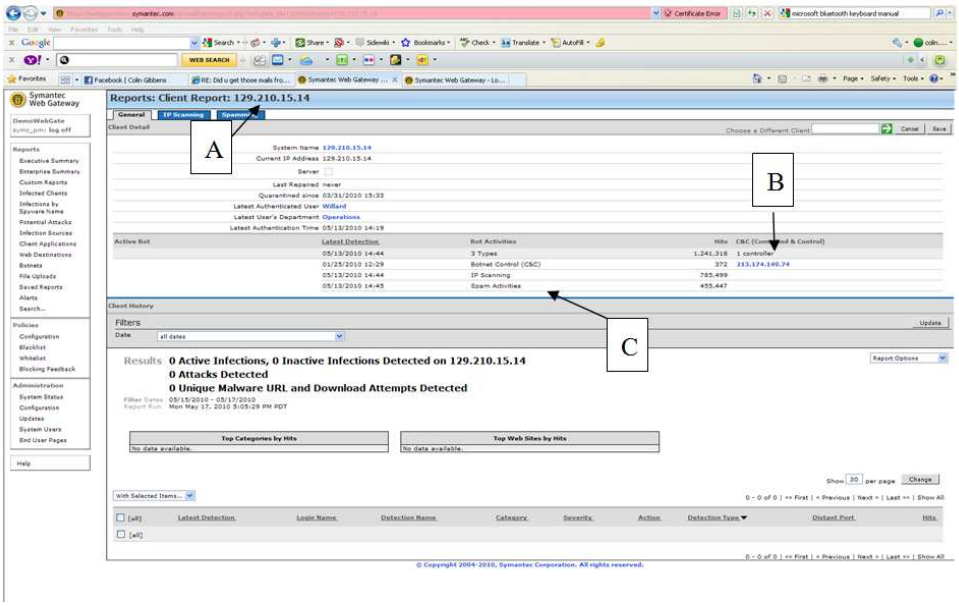
- Will check in with C&C periodically
- Can be months until next activity

In this phase the bot is marked as "Inactive" since the Symantec Web Gateway has not detected any recent bot activity from the system. If the Symantec Web Gateway sees any further bot activity, it immediately changes the status back to "Active."



Investigating Bot Activity

In the following report, The Symantec Web Gateway identifies several systems as “Active” bots. For this classification, we know that The Symantec Web Gateway must have seen several bot behaviors for the system. Clicking on the system from within the Botnet Report allows us to drill down to determine what kind of bot behavior we saw from this system.

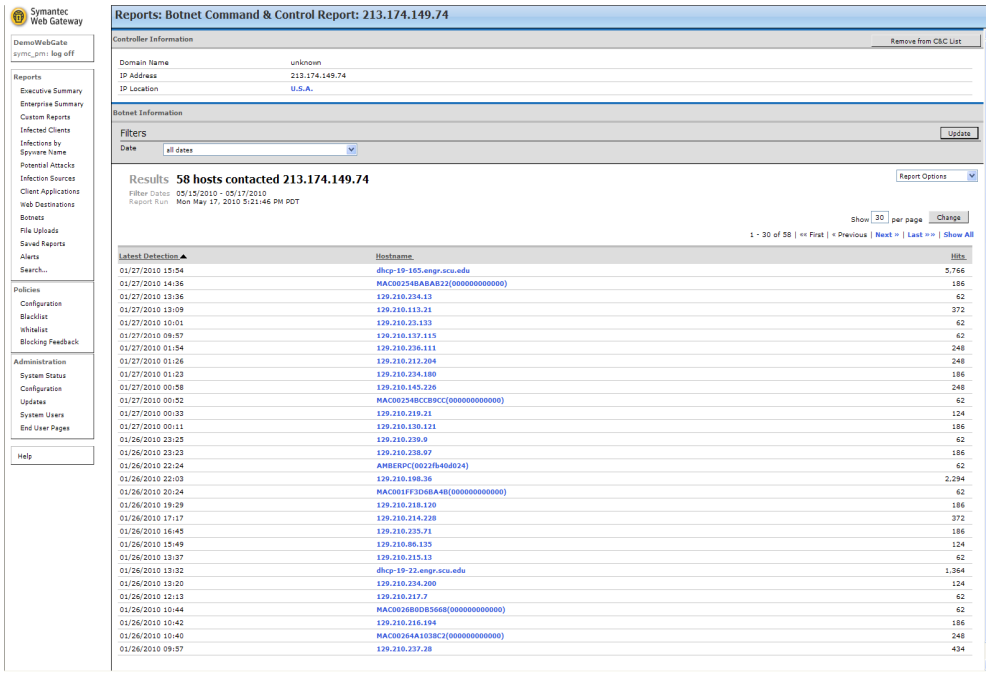


As we drill down, we can determine the following further pieces of information:

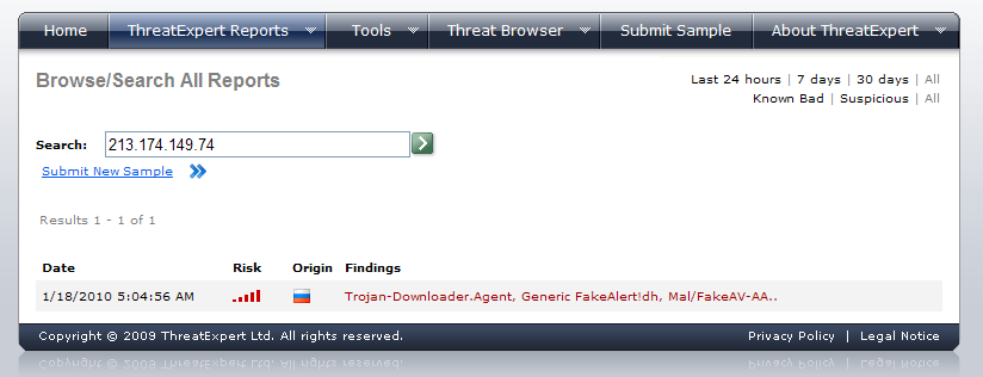
A. The address of the internal system that is compromised
B. The address of the command and control server(s)
C. The behavior that was detected on the system

Potential Behaviors:

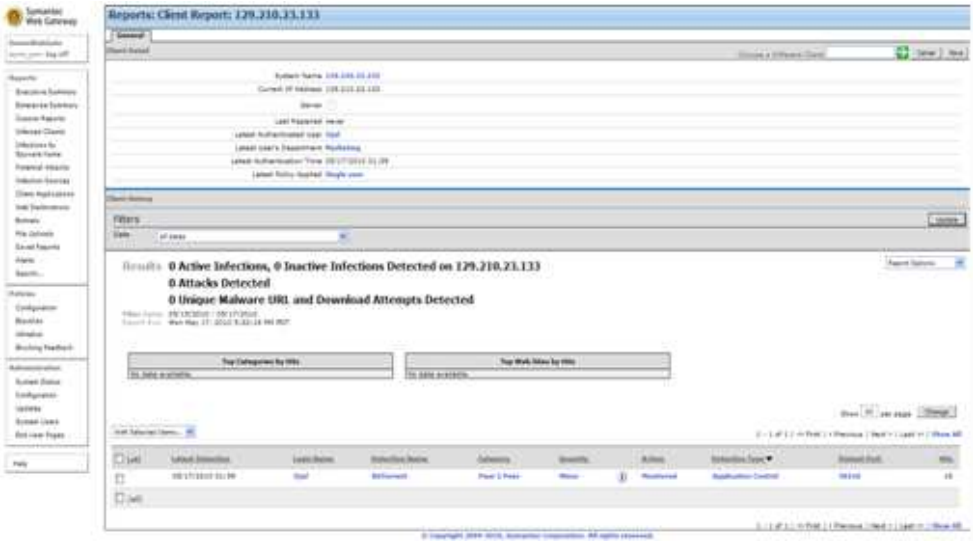
- **Command and Control**—Session was detected from the two systems. By clicking on the IP address of the Command and Control server, we can obtain a list of other systems in the network that were contacted.
- **IP Scanning**—The systems probed for other systems
- Spam Activities—The system generated an unusual amount or pattern of mail messages
- **DDoS**—The computer attempted a denial of service attack on a web server or other computer
- **Phone Homes and Downloads**—The computer attempted to transmit known malware files or used a known phone home pattern.



Using external sources we can identify the malware that was associated with this C&C. Sites that you can use for analysis include **www.threatexpert.com** or **www.safeweb.norton.com**.



Further analysis of an infected system can help us identify other activity, such as websites the compromised system visited or the use of P2P applications that can lead to data leakage or the downloads of malicious apps.

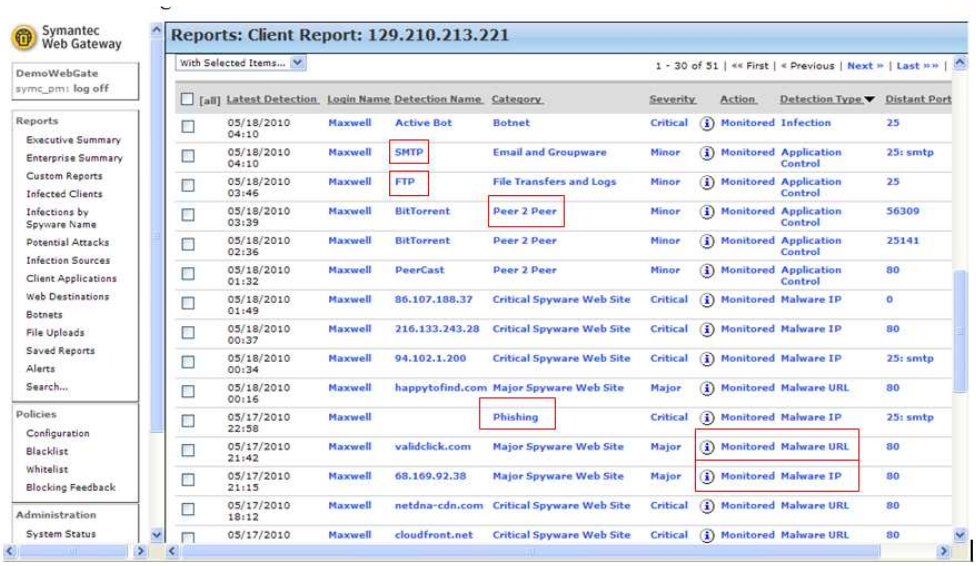


Once a bot is installed on a system, the bot will attempt to connect to the Controller which will issue commands to the zombie computer to be carried out. After finding a system that has been reported in the Botnet Report, further research on activity from that system should be done.

Some things to investigate:

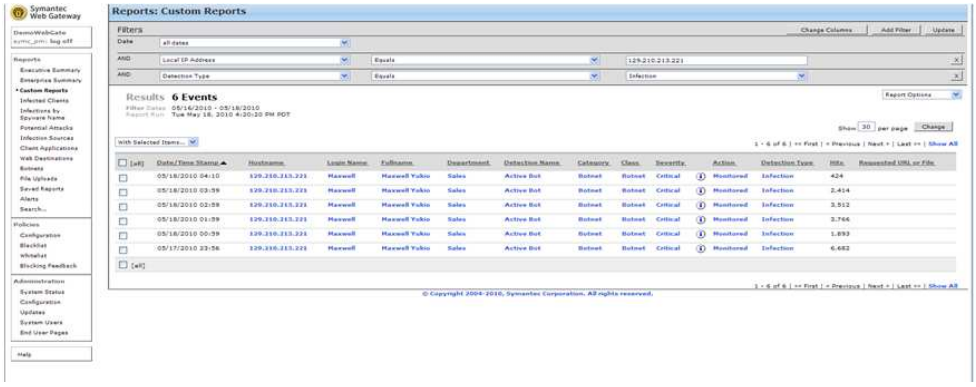
- File uploads and downloads
- Scanning other systems
- Unusual amount of traffic from that system (Spam, Dos)

The following example calls out several activities of interest on this system:



Notice the number of sites that this IP visited that were identified as being either a Malware IP or URL. We can also see signs of phishing activity, as well as a number of P2P connections. The report also detected FTP, as well as SMTP traffic, from this system.

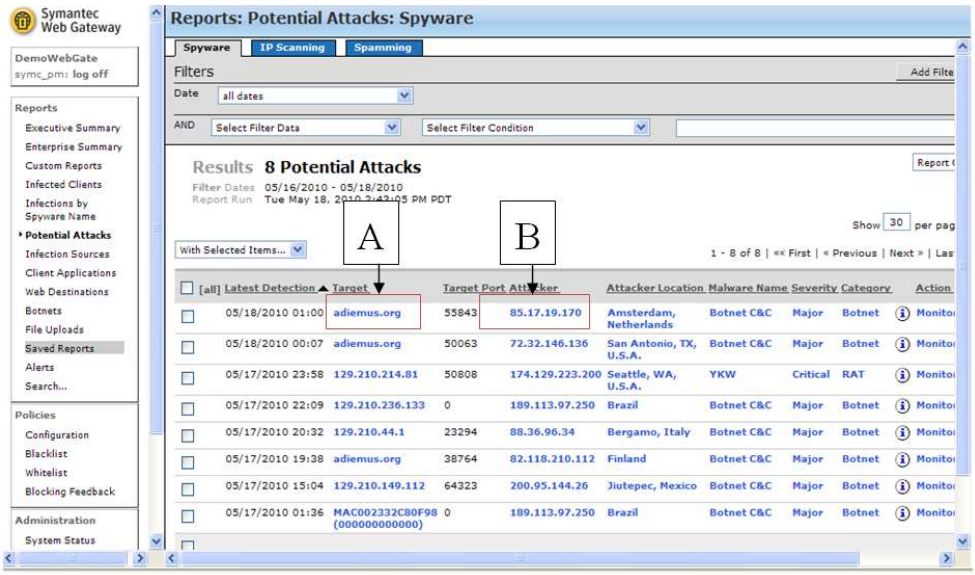
You can also perform further analysis by running a custom report on a potentially compromised system:



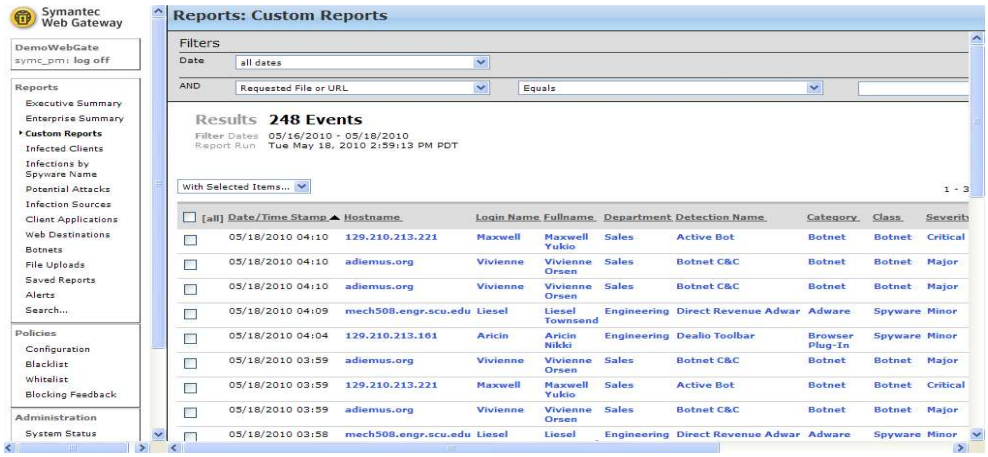
Investigating a Potential Attack

A *potential attack* is an attack that targeted the system but the system was not responsive to the attack or the system was not online. The attack itself penetrated the environment and was detected by The Symantec Web Gateway. Potential attacks are cause for concern because even though the one system was unresponsive to the attack, others might be vulnerable and subject to successful targeting by the attacker.

The following example shows a Potential Attacks report, calling out the target system that was not responsive (A) and the attacker (B).



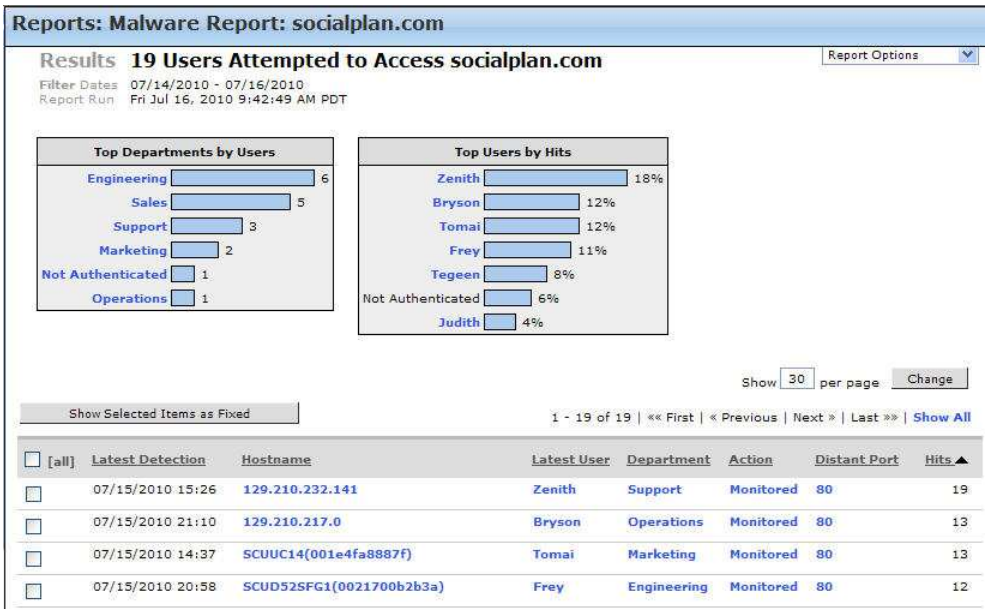
For further analysis, we can click on the attacker's IP address to pull up a listing of other systems that the attacker targeted or were responsive. The following example depicts the results of the query.



Investigating the Top Sources of Infection

Another useful report is the Infection Sources report, which helps identify systems that may be infected with some kind of malware for which signatures may already exist. An example of the report follows.

If you click on a specific Spyware/Malware name, the Malware Report opens. This report shows show the systems recently attempted to access or download a specific piece of Spyware/Malware. You may need to perform further investigation on these systems.



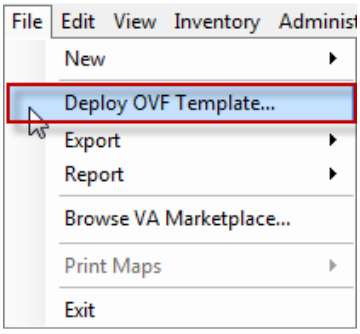
Additional Resources for Malicious Activity Assessments

Resource	Description
Malicious Activity Assessment (MAA) Datasheet	A quick customer-facing overview on the process, benefits, and key results of a Malicious Activity Assessment.
Sales/Partner Cheat Sheet	A one-page overview summarizing how to find and qualify ideal candidates for MAAs.
MAA Pre-Assessment Technical Questionnaire	An environment and prerequisite survey to be completed with the input of customer at least 2 weeks prior to the assessment.
SWG MAA Kick-Off Presentation	A sample presentation template to be customized and delivered to the customer prior to commencement of assessment.
SWG MAA Wrap-up Presentation	A sample presentation template to be report findings to customer following the assessment.
Symantec Web Gateway Version 5.0 Implementation Guide	Technical documentation for the Symantec Web Gateway.
Symantec Internet Security Threat Report: Trends for 2010	Symantec's annual report on the Internet threat landscape, which is full of compelling details and statistics to use in presentation and discussions with the customer. Location: http://www.symantec.com/business/threatreport/index.jsp

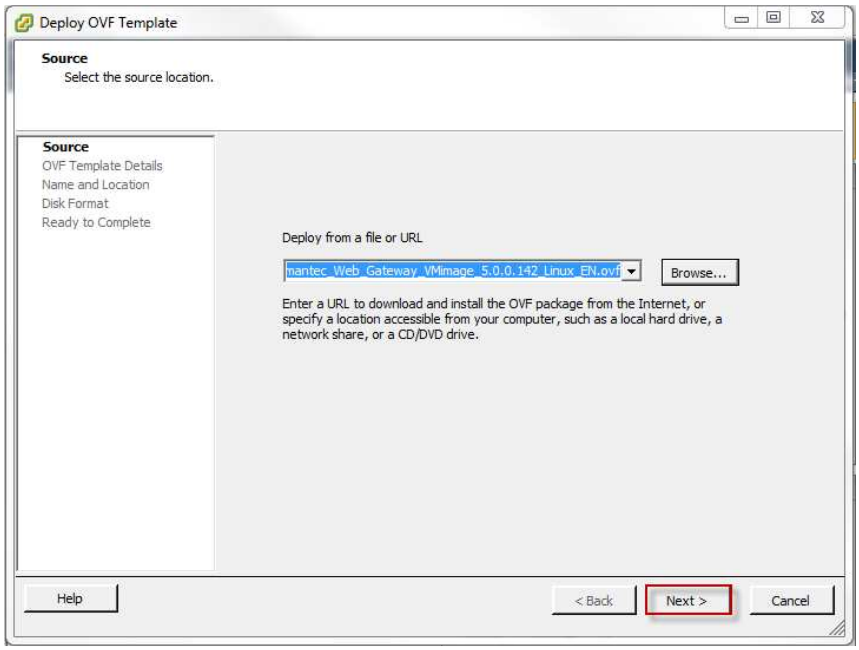
Deploying the Web Gateway on an ESXi V4.x server

The steps below walk through deploying the Web Gateway in a virtual environment for a Malicious Activity Assessment once ESXi V4.x is up and running and you are connected to the serer using the VSphere Client.

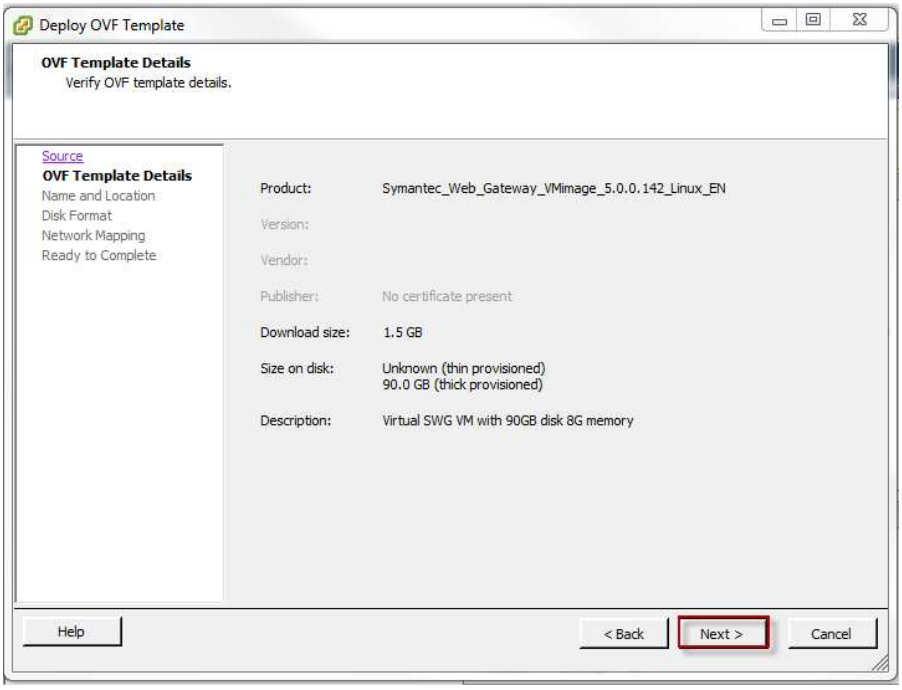
1. From the **File** menu in the vSphere Client select **Deploy OVF Template…**



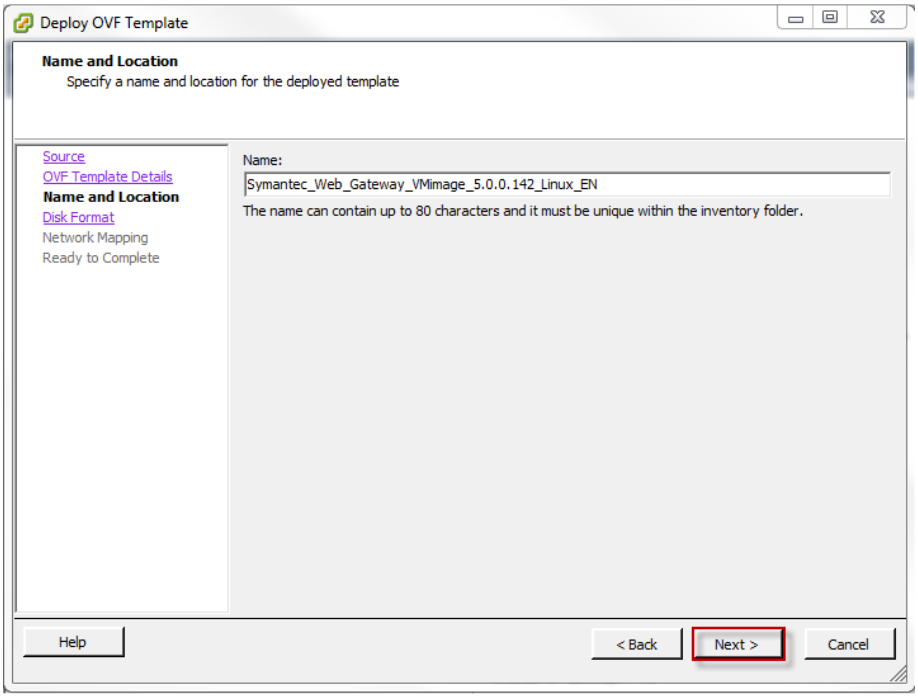
2. Browse to where the virtual image has been downloaded, select and open the images .ovf file and click **Next** to continue.



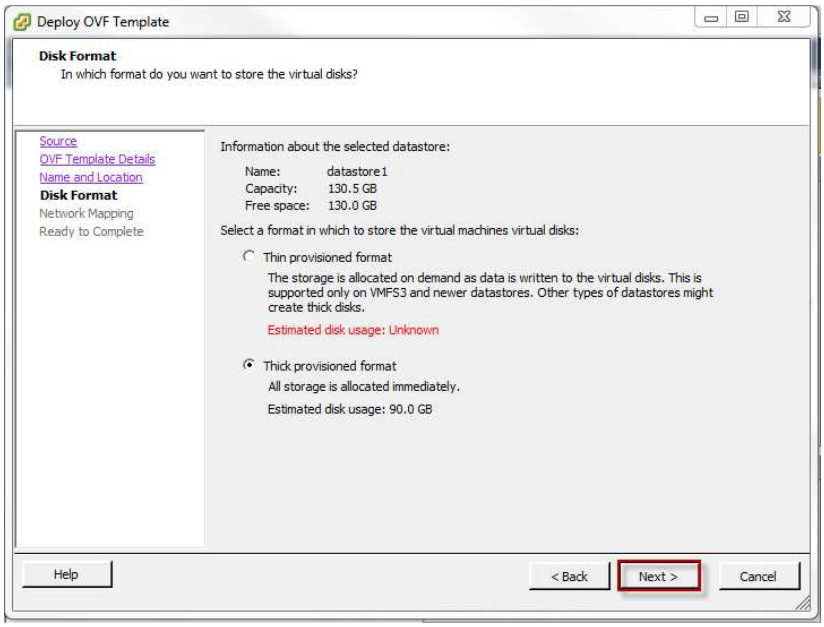
3. Click Next on the OVF Template Details page.



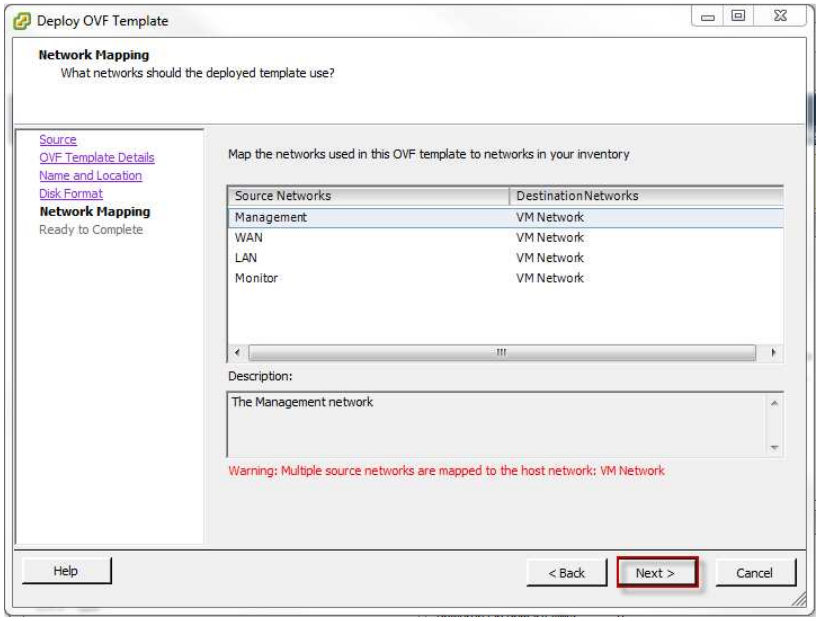
4. Click **Next** on the Name and Location page.



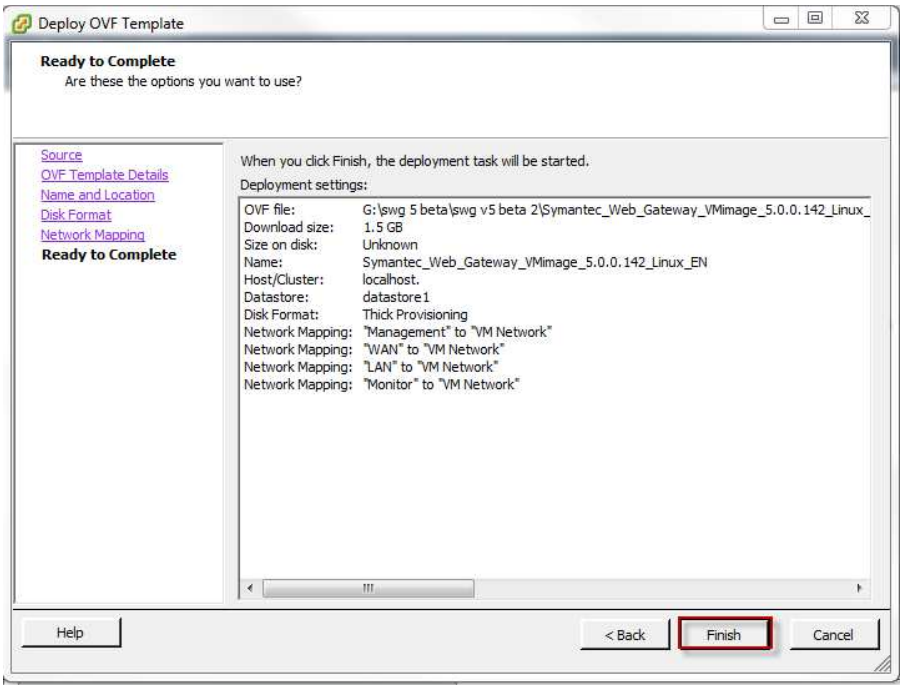
5. Click **Next** on the Disk Format page.



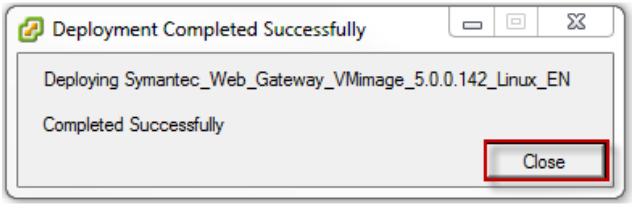
6. Click **Next** on the Network Mapping page.



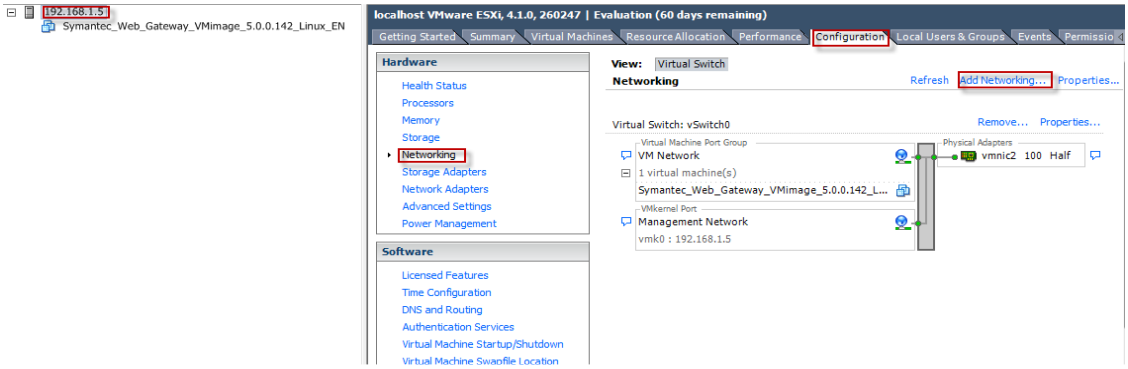
7. Click **Finish** button on the Ready to Complete page.



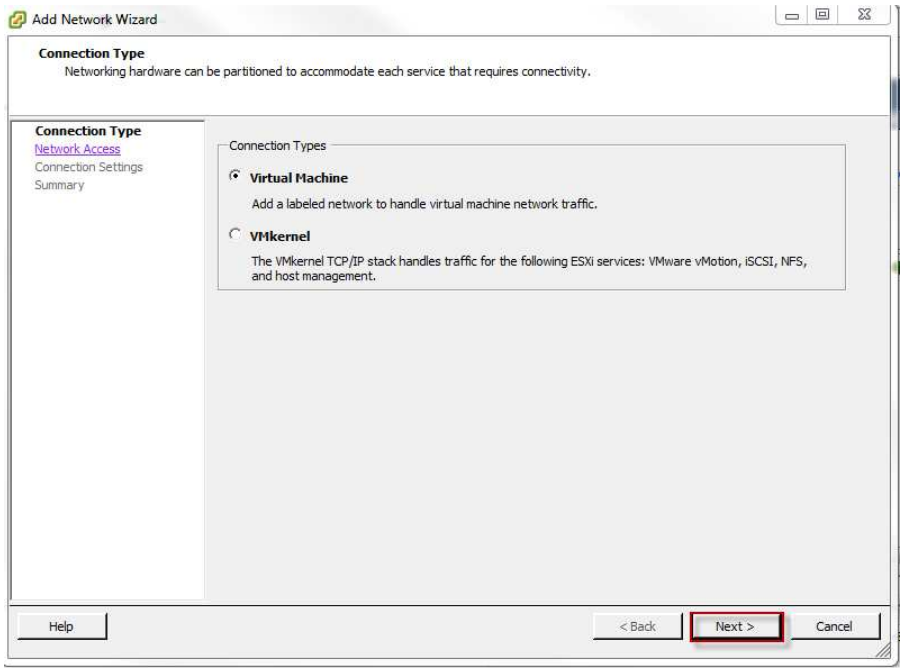
8. It will normally take a few minutes for the image to be deployed to the server. Click Close once you are informed the deployment was successful.



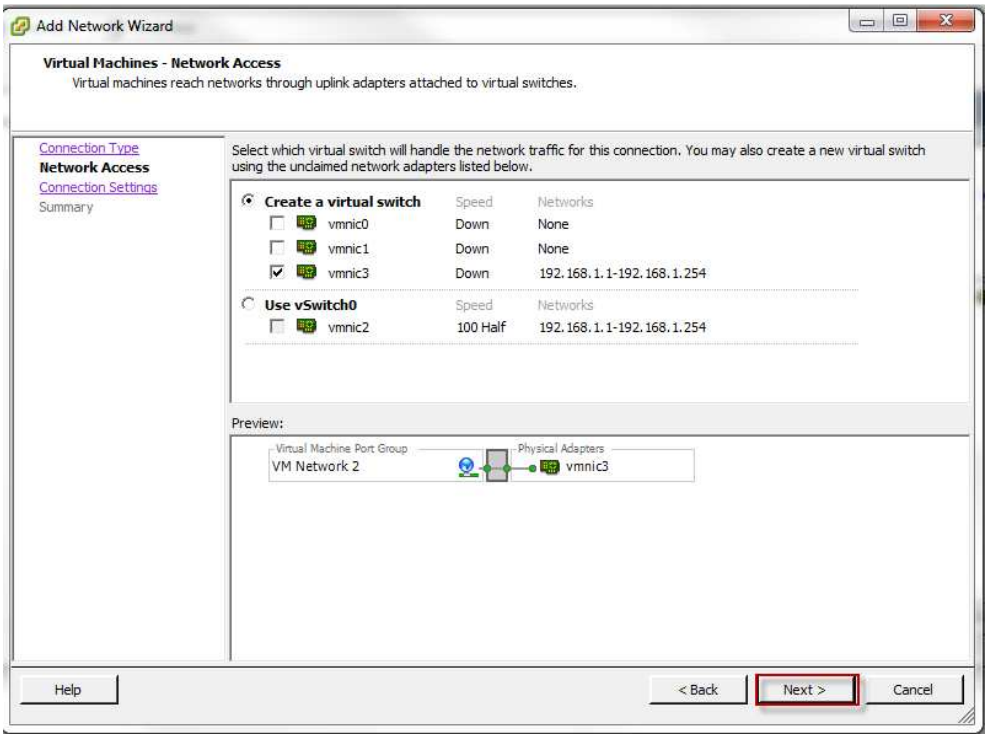
9. Click on the ESXi server in the vSphere client, select the **Configuration** tab, under **Hardware** choose **Networking**, then click the **Add Networking…** link.



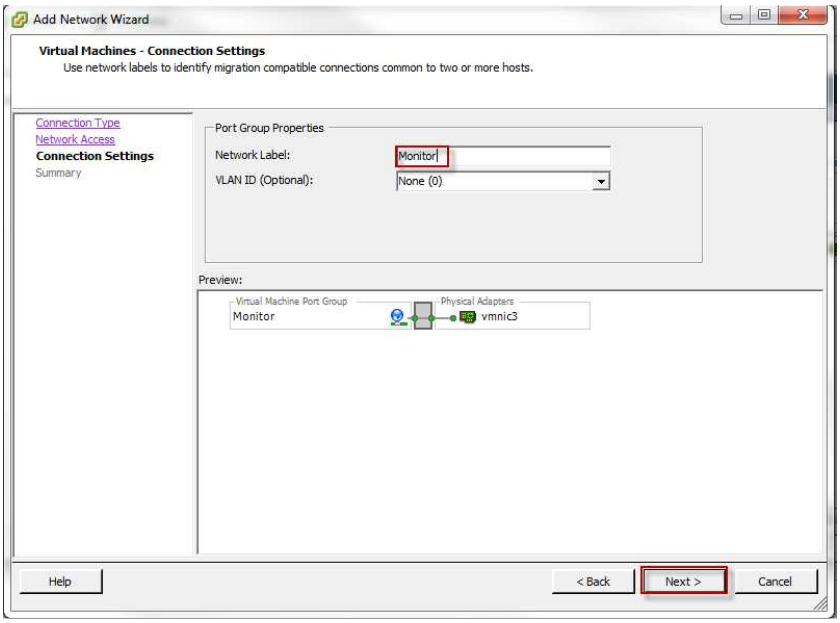
10. Choose the **Virtual Machine** Connection Type, then click **Next**.



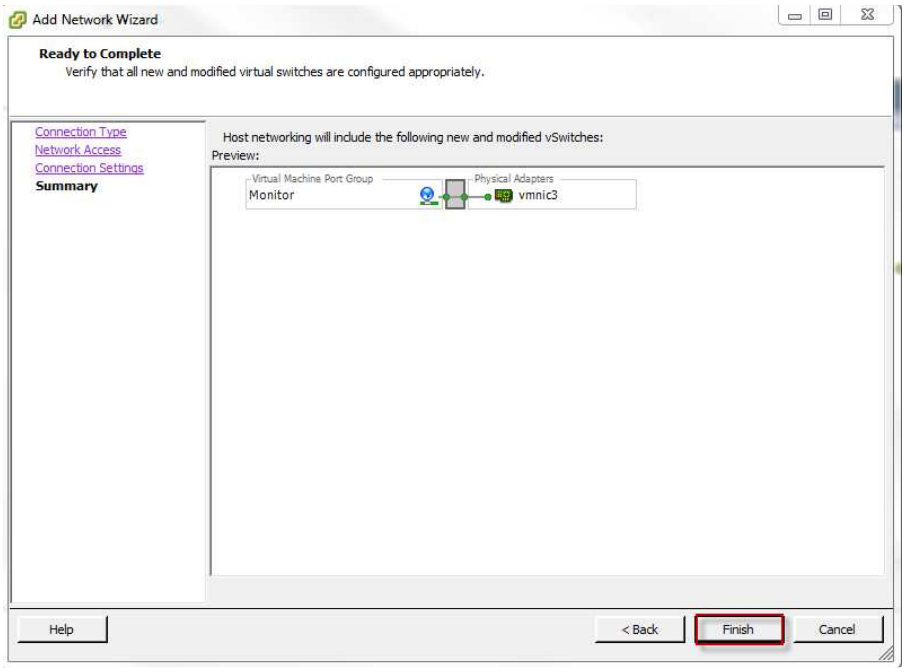
11. Select **Create a Virtual Switch** and choose an available unused interface(In the example I am using the **vmnic3** interface). This will be used as our Monitor interface in the environment. Click **Next**.



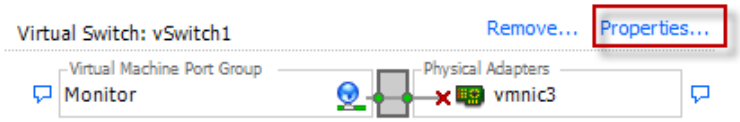
12. Enter **Monitor** as the Network Label. Click **Next**.



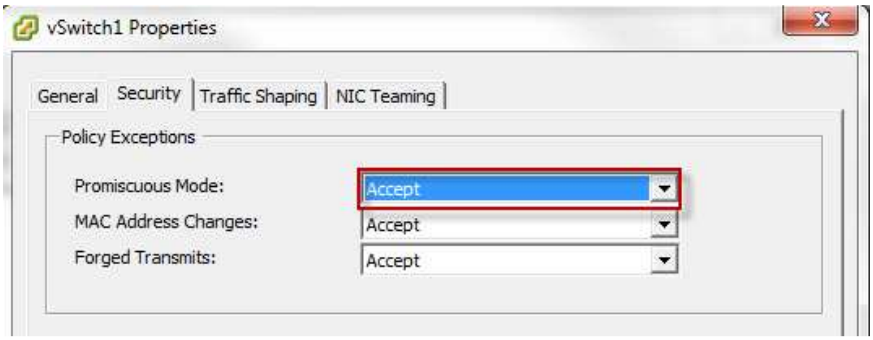
13. Click the Finish button to add the new Virtual Switch.



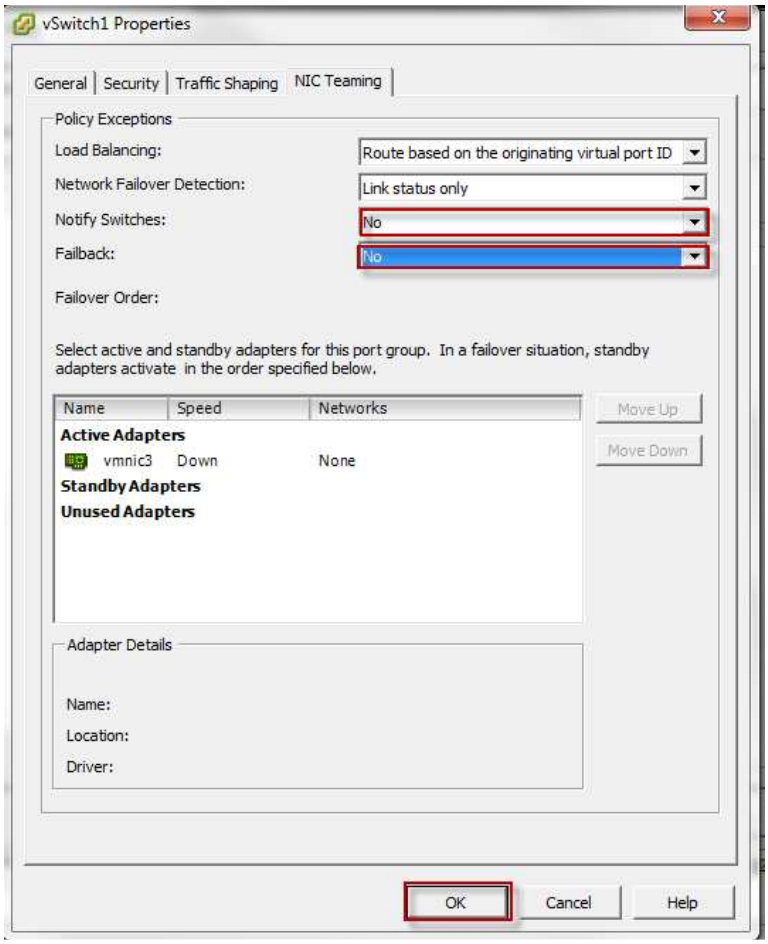
14. Click the **Properties…** link beside the new Virtual Switch.



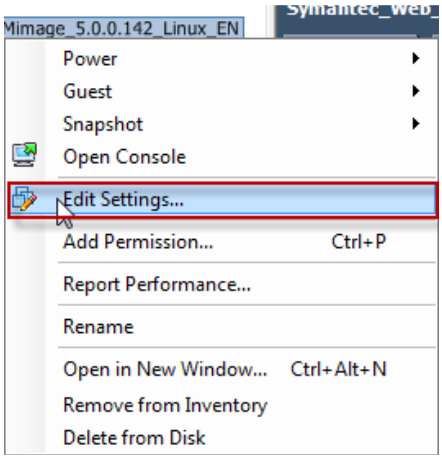
15. Click the **Edit** button on the vSwitch Properties page.
16. Click the **Security** tab and set the Promiscuous Mode dropdown to **Accept**.



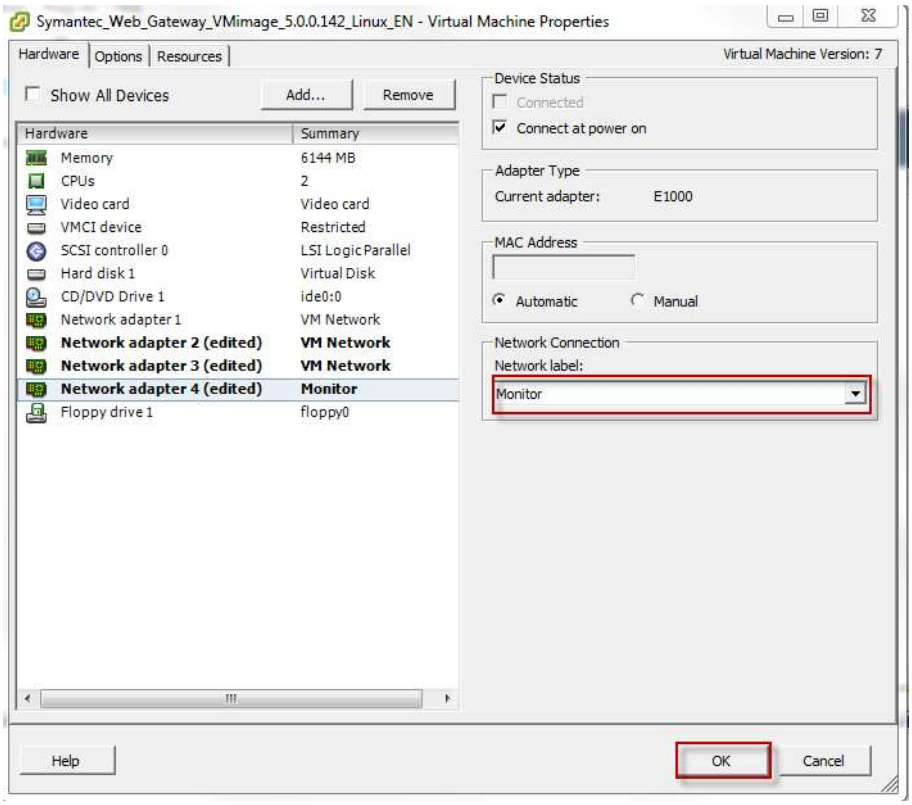
17. Click the **NIC Teaming** tab. Set the Notify Switches and Fallback dropdowns to **No**. Click the **OK** button.



18. Click the **Close** button to close the vSwitch Properties page.
19. Highlight the Web Gateway virtual machine, right click and select **Edit Settings**.

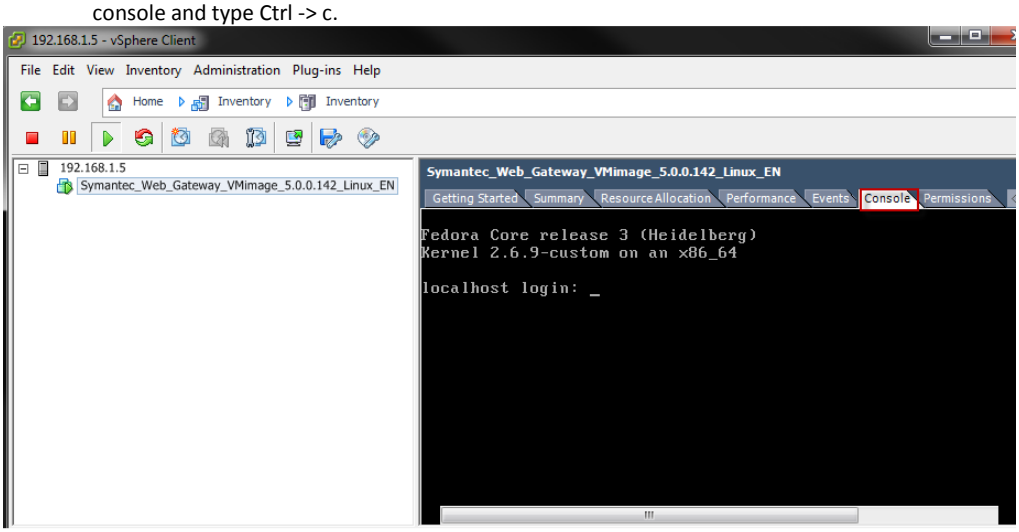


20. Highlight Network Adapter 2 and Network Adapter 3 and uncheck the **Connect at power on** checkbox.
21. Highlight Network Adapter4 and choose **Monitor** from the Network label dropdown. Click the **OK** button.



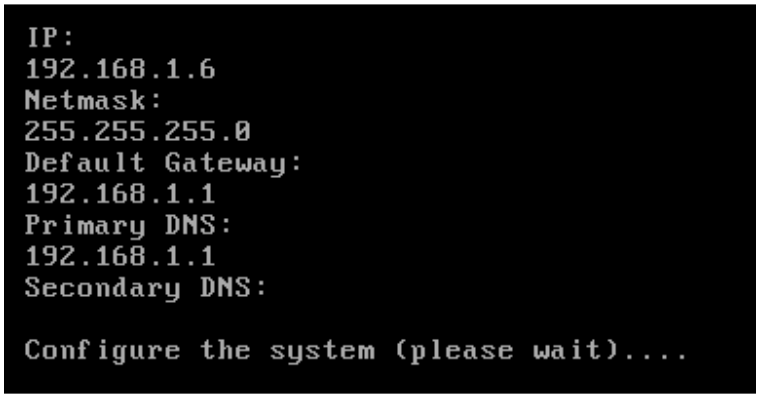
22. Click the **Power On** button to turn on the Web Gateway appliance.

23. Click the **Console** tab to view the Web Gateway booting up. After a few minutes you should see the Fedora login screen. If you see any type of error on the login page, click inside the console and type Ctrl -> c.



24. Login with the username '**admin**' and password '**admin1!**'. Choose **5** from the menu to '**Change/Test IP configuration**'.

25. Select 3 to 'set IP/disable DHCP'.
26. Enter the IP, Netmask, Default Gateway and DNS server(s)that will be used by the Management interface on the network(this IP should be on the same network as the ESXi server). After a few moments the Web Gateway will take on its new IP.



27. From this point on you can follow the instructions starting at step 3 in the 'Setting up the Symantec Web Gateway for a Malicious Activity Assessment' section of this document. You can make the initial connection to the IP address that was just assigned to the Web Gateway instead of the default IP of 192.168.254.254. You also won't need to adjust the IP when you reach step 8. When all configuration is finished and it's time to put the Web Gateway into production, in this situation we don't need to worry about the management interface as it is already cabled(this is the same cable connecting the ESXi server to the network). A cable from the Span Port or Network Tap now needs to be connected to the interface assigned to the Virtual Switch we created. At this point the Web Gateway should be monitoring network traffic.

About Symantec Corporation

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif. , Symantec has operations in 40 countries. More information is available at www. symantec. com.

For specific country offices and contact numbers, please visit our Web site.

For product information in the U. S. , call toll-free 1 (800) 745 6054.

Symantec Corporation

World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www. symantec. com