Guide for Configuring, Monitoring and Troubleshooting the Network Inspection System (NIS) in Forefront Threat Management Gateway (TMG) 2010

Authors and Contributors

Authors

Avi Ben-Menahem, Microsoft

Tanmay Ganacharya, Microsoft

Moshe Golan, Microsoft

Ziv Mador, Microsoft

Evgeney Ryzhyk, Microsoft

Contributors

Tom Bolt, Microsoft (Liane Morley Marketing LLC)

Jim Harrison, Microsoft

Adwait Joshi, Microsoft

Scott Lambert, Microsoft

Vladimir Lifliand, Microsoft

Duane Okamoto, Microsoft

Eli Pozniansky, Microsoft

Evgeny Skarbovsky, Microsoft

Jeff Williams, Microsoft

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Contents

Overview

Microsoft Threat Management Gateway 2010 Overview

Microsoft® Forefront™ Threat Management Gateway 2010 (TMG) is the next generation release of ISA Server 2006. Forefront TMG allows employees to safely and productively use the Internet without worrying about malware and other threats. It provides multiple layers of continuously updated protections against the latest Web-based threats, including URL filtering, antimalware inspection, and intrusion prevention. These technologies are integrated with core network protection features to create a unified, easy-to-manage gateway that reduces the cost and complexity of Web security. Forefront TMG enables organizations to perform highly accurate Web security enforcement by stopping employee access to dangerous sites based on reputation information from multiple Web security vendors and the technology that protects Internet Explorer 8 users against malware and phishing sites. Forefront TMG provides:

Comprehensive Protection:

- **Blocks malicious sites more effectively.** Forefront Threat Management Gateway improves blocking of malicious sites using aggregated data from multiple URL filtering vendors and the antiphishing and malware technologies that also protect Internet Explorer 8 users.
- **Prevents exploitation of vulnerabilities.** Forefront Threat Management Gateway provides integrated intrusion prevention technology that protects against browser-based and other vulnerabilities, including browser plug-in exploits.
- **Catches Web-based malware.** Forefront Threat Management Gateway provides highly accurate malware detection with a scanning engine that combines generic signatures and heuristic technologies to proactively catch variants without specific signatures.
- **Combines secure Web gateway with core network protection.** Forefront Threat Management Gateway integrates core network protection technologies from Internet Security & Acceleration Server 2006, the previous version for Forefront Threat Management Gateway 2010. These proven technologies allow customers to also deploy a perimeter firewall or a secure gateway for applications such as Exchange, SharePoint and Web servers.

Integrated Security

- **Integrates multiple Web defenses in a single solution.** Forefront Threat Management Gateway integrates URL filtering, reputation services, antimalware, intrusion prevention, Web proxy and HTTP/HTTPS inspection on a single server.
- **Reduces costs.** Customers who purchase Forefront Threat Management Gateway can save on capital expenditures by deploying the solution as a virtual machine.
- **Integrates with existing infrastructure.** Forefront Threat Management Gateway simplifies authentication and policy enforcement by integrating with Active Directory. For example, it

simplifies HTTPS inspection by distributing its certificate via Active Directory. It also leverages Windows Update infrastructure to enable quick distribution of new protection to all Forefront Threat Management Gateway servers.

Simplified Management

- **Provides centralized management.** Forefront Threat Management Gateway allows administrators to create and manage all Web security functions across distributed environments from a single console.
- **Delivers comprehensive, custom reports.** Forefront Threat Management Gateway generates Web security reports quickly and allows administrators to easily customize to meet business-specific reporting needs. It also integrates with SQL Server Express or existing SQL infrastructure to create custom reports.

For more information about Forefront TMG, please visit **www.microsoft.com/TMG** or refer to the help file which is provided with the product.

Microsoft NIS Overview

As information workers increasingly rely on Internet access for their work, ubiquitous and comprehensive protection is paramount, regardless of what application or protocol are used. End users predominately access the Internet using Web browsers which creates a common attack surface for hackers. The nature of the Web demands protections against "over the wire" exploits using the frequently used HTTP protocol as well as other protocols that various applications may use such as RPC, SMB and several email protocols. This protection helps optimize the user experience when provided by the gateway on the network edge or between network segments. Network Inspection System (NIS) is Microsoft's response to this new and growing IT concern. In its first release, NIS is integrated in Forefront TMG as a component of its Intrusion Prevention System (IPS) offering.

Given the large number of application-level protocols and new ones constantly emerging, Microsoft Research (MSR) architected Generic Application-level Protocol Analyzer (GAPA), consisting of a protocol specification language (GAPA Language: a.k.a. GAPAL) and an analysis engine that operates on network streams and captures[1]. GAPA allows rapid creation of protocol parsers, greatly reducing the development time needed. In Forefront TMG, we have implemented NIS, based on the GAPA research, as a signature-based network Intrusion Prevention System (IPS).

With continuous zero-day attacks that are carried out over the network, Microsoft constantly looks for ways to protect networks against exploitation of the discovered vulnerabilities. One of the key problems is that attackers can usually develop and use exploits for the disclosed vulnerabilities faster than software vendors can develop security updates and customers can test and deploy those updates. Reviewing past vulnerabilities shows that it often takes a month or longer from the initial attacks reports to develop and release the security update, and on top of that, several days or weeks (or even longer) for customers to test and deploy the update across their networks. This leaves computers vulnerable to

[1] See the Microsoft Research paper: http://research.microsoft.com/pubs/70223/tr-2005-133.pdf

attacks and exploitation for a substantial period. The main purpose and value proposition of NIS is to greatly reduce the vulnerability window between vulnerability disclosures and patch deployment from weeks to a few hours. The vulnerability research and the signature development are done by the world-class Microsoft Malware Protection Center (MMPC). The MMPC releases NIS signatures for newly released Microsoft bulletins when applicable, on the day the bulletins are released as well as for various zero day issues. For those bulletins that fix publicly-unknown vulnerabilities, NIS helps provide a nearly-immediate protection shortly after the details of the vulnerability become publicly known through the bulletin release. MMPC also provides fast response to zero day incidents by releasing NIS signatures for these issues as soon as they become known. At this time, NIS signatures help detect exploits of vulnerabilities in Microsoft products only.

Let's review a common vulnerability discovery scenario, regardless whether it was part of a zero day incident or a bulletin release.

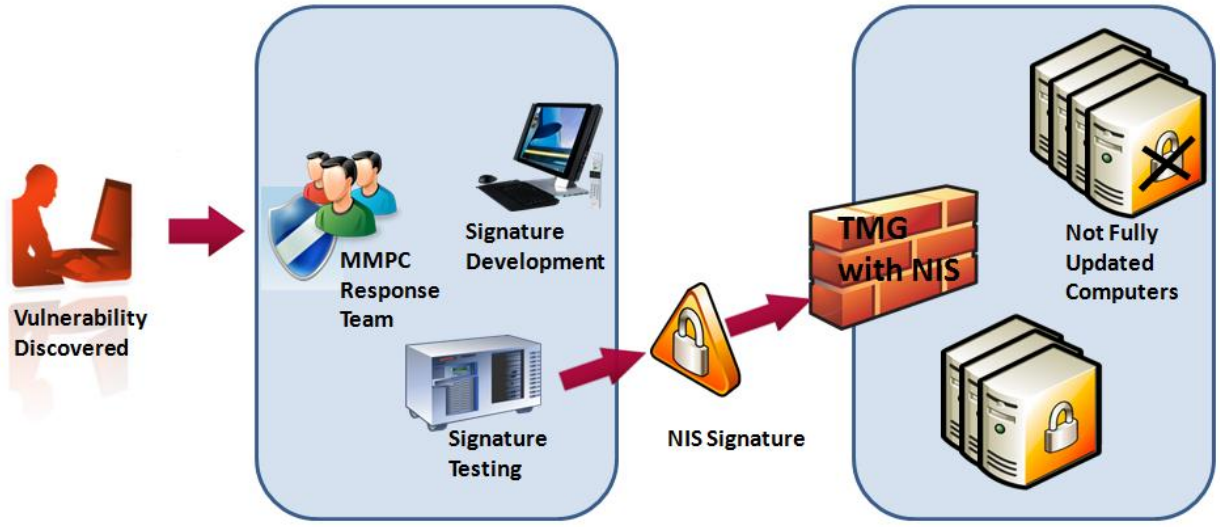


Figure 1: NIS protecting organizations from exploits of discovered vulnerabilities

1. Vulnerability discovery: The MMPC leverages a variety of tools and technologies to monitor and search for new exploits for known and unknown vulnerabilities.
2. Once such vulnerability discovered, MMPC researchers begin the analysis and the signature development. The signature also passes through rigorous automated testing.
3. When the research team completes the signature development and testing, it is published through the Microsoft Update service. Customers can also use Windows Server Update Services (WSUS) to distribute these updates to their TMG servers.
4. Forefront TMG automatically downloads and installs the new signatures, if configured so.

Please refer to the Understanding the Research and Response for NIS section for more details about how the MMPC analyzes and responds to emerging threats.

NIS Signature Types

NIS provides protection by using three different types of signatures:

1. **Vulnerability-based:** These signatures will detect most variants of exploits against a given vulnerability.
2. **Exploit-based:** These signatures will detect a specific exploit of a given vulnerability.
3. **Policy-based**: These signatures that are generally used for auditing purposes and are developed when neither vulnerability nor an exploit-based signature can be written.

Exploring NIS Components

General Architecture

NIS is a multi-component system that helps detect many attacks which involve exploits of software vulnerabilities. The following section provides details about the architecture of NIS.

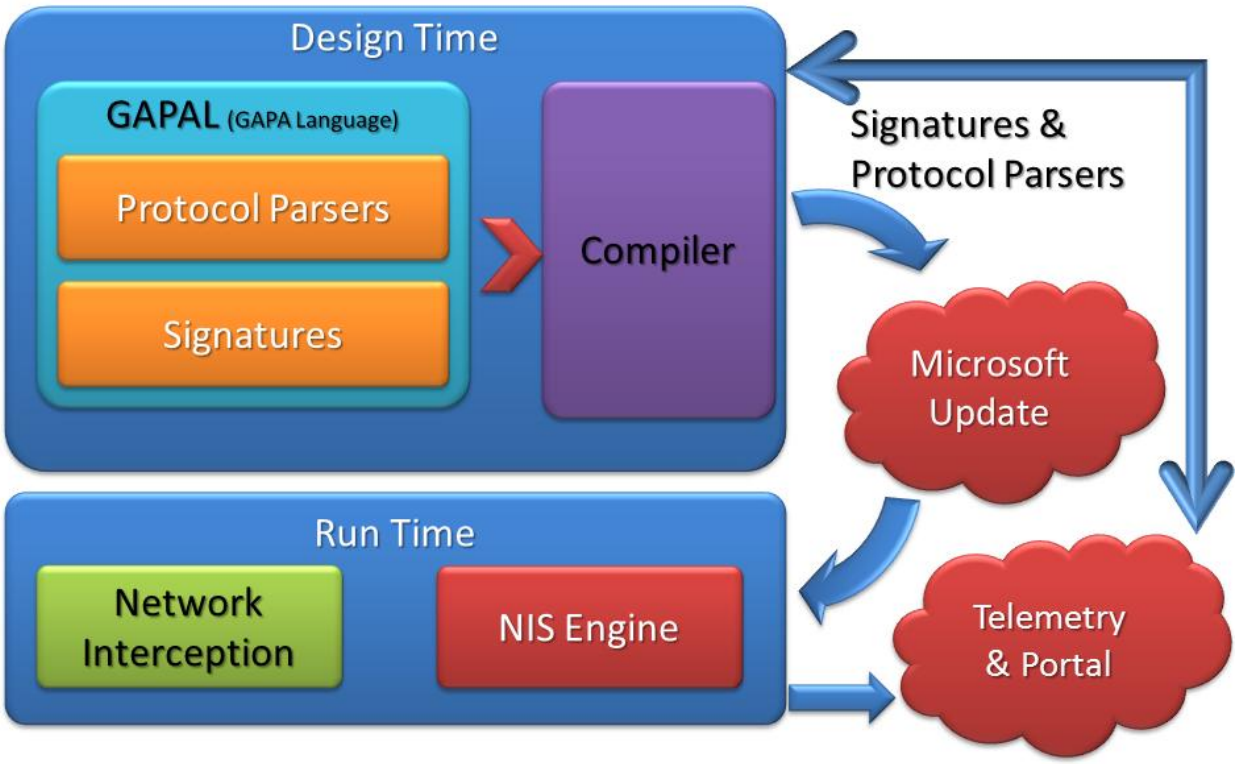


Figure 2: NIS conceptual architecture

GAPA Language (GAPAL) and Compiler

Traditional network protocol parsers are coded using certain imperative language such as C or C++. These parsers usually read the packet bytes in a sequential manner, executing some logic in-between to determine the required actions. At the heart of GAPA lies the GAPA Language (GAPAL) – a declarative language with imperative elements, designed for protocol parser development. The language has

constructs and concepts specific to the domain of network and application protocol parsing. GAPA's approach is to combine imperative and declarative styles, while shifting as much protocol parsing logic as possible to the declarative part.

A typical network protocol is described using the format of various messages passed between the client and the server, and by the semantic relations between those messages. GAPAL provides the means to specify both the protocol "grammar" – that is, the message format, as well as the protocol "state machine" – the expected sequence of messages as seen by the man-in-the-middle inspecting the traffic.

NIS functionality is defined by a signature. A NIS signature is a collection of code blocks attached to the protocol parser that detect attempts to exploit known vulnerabilities "over the wire" by reacting to various parsing events and examining the parser state

As an example, here's the simplified HTTP protocol definition in GAPAL:

```
protocol Http
{
    set parentid = TCP;
    set InterceptionType = "Network";
    set ConnectionType = "TCP";
    set PortsRange = "80";

    grammar
    {
        {
            string RequestUrl;
            uint32 ContentLength;
        }

        %%

        HttpMessage -> Request | Response;
        Request -> RequestLine HeadersAndBody;
        Response -> ResponseLine HeadersAndBody;
        RequestLine ->
            Method
            uri:"[^ \t\r\n]+"
            {%
                RequestUrl.Set(uri);
            %}
            "HTTP/1.1\r\n";
        Method -> "GET" | "POST" | ...;
        ResponseLine -> "HTTP/1.1 " statusMessage:".*\n";
        HeadersAndBody -> Headers Body;
        Headers -> Header Headers | "(\r\n)";
        Header -> ContentLengthHeader | ... ;
        ContentLengthHeader ->
            "Content-Length:[ \t]*"
            lengthStr:"[0-9]+"
            {%
                ContentLength = lengthStr.ParseNumber();
            %}
```

```
            ".*\n";
        Body -> uint8<ContentLength>;
    }
}
```

Here is an example for a simplified signature that uses that HTTP protocol definition:

```
signature MyHttpSig
{
    set parentid =  Http;

    visitors
    {
        EXPLOIT_PATTERN = ".*bad.*";
        %%
        visitor RequestLine.uri
        {%
            if (RequestUrl.Match(EXPLOIT_PATTERN))
            {
                GapaSignatureMatch();
            }
        %}
    }
}
```

The protocol and signatures definitions are compiled into the low-level binary form by the GAPA compiler. The result of the compilation is a set of parser tables and compiled code blobs packaged in the NIS signature set, which is executed by the NIS engine at run time.

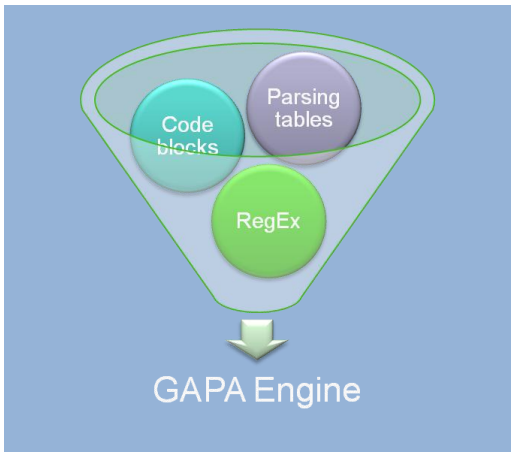


Figure 3: Input components for the GAPA engine

The GAPA Compiler produces:

- A set of regular expression groups indicating how to tokenize the input stream
- Parsing tables dictating how the parse tree is assembled
- Code blocks defining whatever complex logic needed

These inputs are consumed by the GAPA engine for the actual parsing and inspection.

Run Time Architecture

The NIS runtime architecture includes integration of the GAPA engine in multiple traffic inspection points:

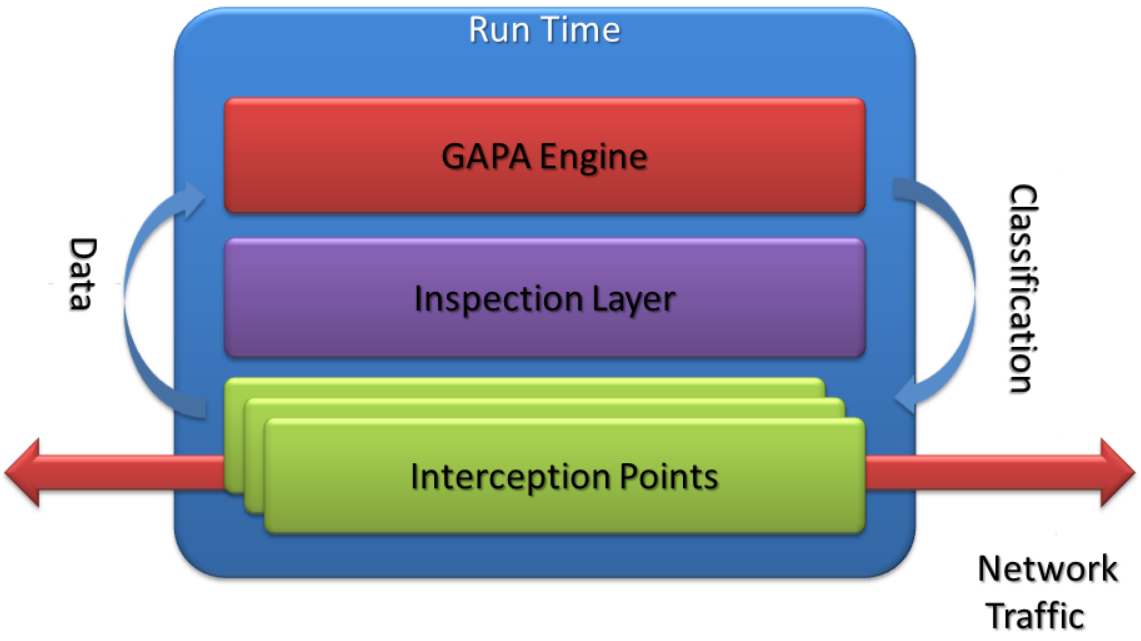


Figure 4: NIS runtime architecture

GAPA Inspection Engine

The GAPA engine is responsible for the actual parsing of the traffic and invocation of the signature code according to the protocol definition and the signature configuration. Conceptually, the engine consists of a low-level pattern matching component (directly exposed to the network stream) and high-level parser which chooses the next pattern to match based on the previously matched pattern and the overall session state.

The GAPA engine provides a low-level platform and services for the protocol parsers. The functions of the engine are:

- Stream buffering and accumulation (when needed)
- Efficient stream decoding and canonicalization functions
- Regular expression matching
- Storage and handling of variables
- Execution of the code blocks
- Protocol layering support

A unique engine instantiation resides in each traffic inspection point, provided with the up-to-date policy set. Engine policy set contains the compiled protocol definitions and signatures. The policy set contains only protocols and signatures relevant to the current interception point for performance optimization.

The GAPA engine default policy is stored in the NIS signature set in a hierarchical structure, supporting protocol layering and protocol extensions. The protocol extension shown on the following figure is an example of layered protocols.

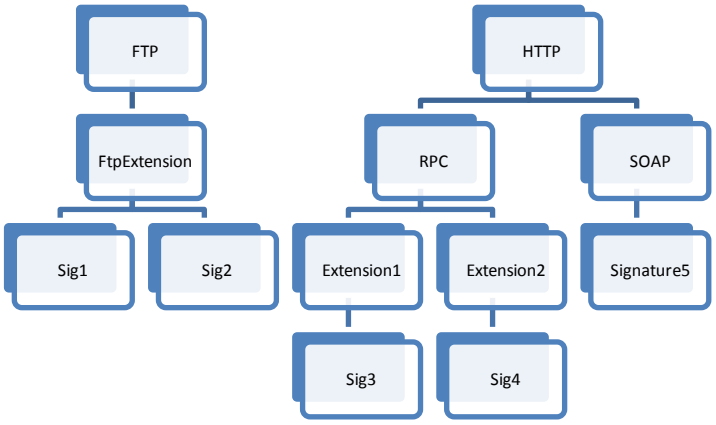


Figure 5: Example for layered protocols and protocol extensions in NIS signature set

In addition to the protocols, the signature set contains signatures and their metadata as well as the GAPA engine binary.

Supported Protocols

NIS can intercept a variety of network protocols that may be used to carry out an attack. Some protocols are used more commonly than others for such attacks. At the publish date of this whitepaper, NIS supports the following protocols:

- HTTP
- DNS
- SMB
- SMB2
- NetBIOS
- MSRPC
- SMTP
- POP3
- IMAP
- MIME

By supporting these protocols, NIS helps provide protection against attacks that happen over Web, mail and file sharing.

As part of the research and response to emerging threats, we constantly evaluate the need for supporting additional protocols and will add that support as necessary. Support for additional protocols will be provided using NIS signature sets. If configured to do so, TMG will automatically download and install the new signature sets and no further action is required by the administrator. In most cases, support for a new protocol is added because there is a significant vulnerability or exploit that uses that protocol, and therefore in most cases, the MMPC will also release a signature that uses that new protocol. You can see what protocols the signatures use, by grouping the NIS signatures by protocol. See the Deciding What Network Traffic to Inspect section for more details.

Signature and Engine Updates

The set of available protocol parsers, the GAPA engine and the signatures are packaged into a **NIS signature set**. Forefront TMG Update Center is responsible for keeping the NIS signature set up to date using the Microsoft Update service. When the new version of a signature set is available, it is downloaded and applied to Forefront TMG NIS. Please see more details in the Configuring NIS section.

Telemetry Service

This section provides details about the Microsoft Telemetry Service in Forefront TMG. See the Configuring Telemetry section for more details.

What This Feature Does

When Forefront TMG identifies potential malware it reports to Microsoft information about the potential attack identified. This information is stored by Microsoft and analyzed to help identify attack patterns and improve precision and efficiency of threat mitigations. Microsoft uses this analyzed information to report on top potential threats in the global network. The information collected is not used to identify or contact you.

Information Collected, Processed, or Transmitted

The information collected by Microsoft includes the traffic triggering the potential threat and the potential threat identified, such as protocol information, file names, cryptographic hash, vendor, size, and date stamps. In addition, if you choose advanced membership, Microsoft will collect more extensive diagnostic information, including traffic samples and full URLs to help indicate the origin of the file or traffic. This additional information may inadvertently contain personal information such as search terms or data entered in forms, but this information will not be used to identify or contact you. We may also collect a record of the actions you applied when a potential threat was detected (deny or permit). Microsoft collects this information to help Microsoft gauge the effectiveness of Forefront TMG's ability to mitigate malware attempts and to provide you and other users' information on top potential threats.

Forefront TMG will also send report to Microsoft automatically when:

- Forefront TMG detects software or changes to your computer by software that has not yet been analyzed for risks.
- You apply actions to software that Forefront TMG has detected.
- Forefront TMG completes a scheduled scan and automatically applies actions to software that it detects, according to your settings.

You can join Microsoft Telemetry Service with a basic or an advanced membership.

Basic Membership

As a basic member, reports collected by Microsoft from you include standard computer information as well as threat identifier, source and destination IP and Port, a one-way hash of the traffic data, and a globally unique identifier (GUID) to uniquely identify your computer.
The GUID is a randomly generated number; it does not contain any personal information.

Advanced Membership

In addition to the information in the basic membership, if you are an advanced member, the reports collected from you by Microsoft include additional data such as full URL strings and Internet traffic samples captured by Forefront TMG.
Reports may unintentionally contain personal information. To the extent that any personal information is included in a report, Microsoft does not use the information to identify you or contact you.
To help protect your privacy, Microsoft Telemetry Service reports that are sent to Microsoft are encrypted using Secure Sockets Layer (SSL).

Use of Information

These reports, along with reports from other Forefront TMG users who are participating in Microsoft Telemetry Service, help Microsoft researchers discover new threats more rapidly and optimize known threat mitigations.

The reports may also be used for statistical or other testing or analytical purposes, trending, and anti-malware definition generation.

Choice/Control

You can update or cancel your Microsoft Telemetry Service membership at any time. To change your Microsoft Telemetry membership, use the options provided in the Telemetry Participation Setting available on the Properties of any array name by right clicking the name. See the Configuring Telemetry section for more details.

NIS Encyclopedia

The write ups for NIS signatures are included in the online anti-malware encyclopedia on the Microsoft Malware Protection Portal at http://www.microsoft.com/security/portal. It is a great resource for any threat related information, in particular for NIS signatures. The properties page for each NIS signature in

the Forefront TMG User Interface, includes a direct link to the corresponding write up. The text on the link is “More information about this NIS signature online”. You can click it to learn more about the specific signature.

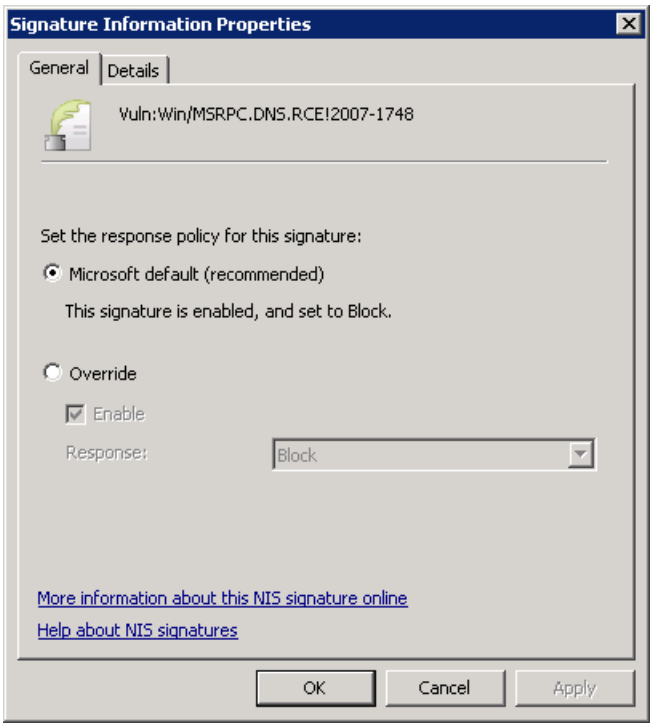


Figure 6: Signature Information Properties page

For example, the link for the Vuln:Win/MSRPC.DNS.RCE!2007-1748 signature is:

http://www.microsoft.com/security/portal/Threat/Encyclopedia/NIS.aspx?threat=Vuln-Win-MSRPC-DNS-RCE-2007-1748

Here is the corresponding encyclopedia write up:

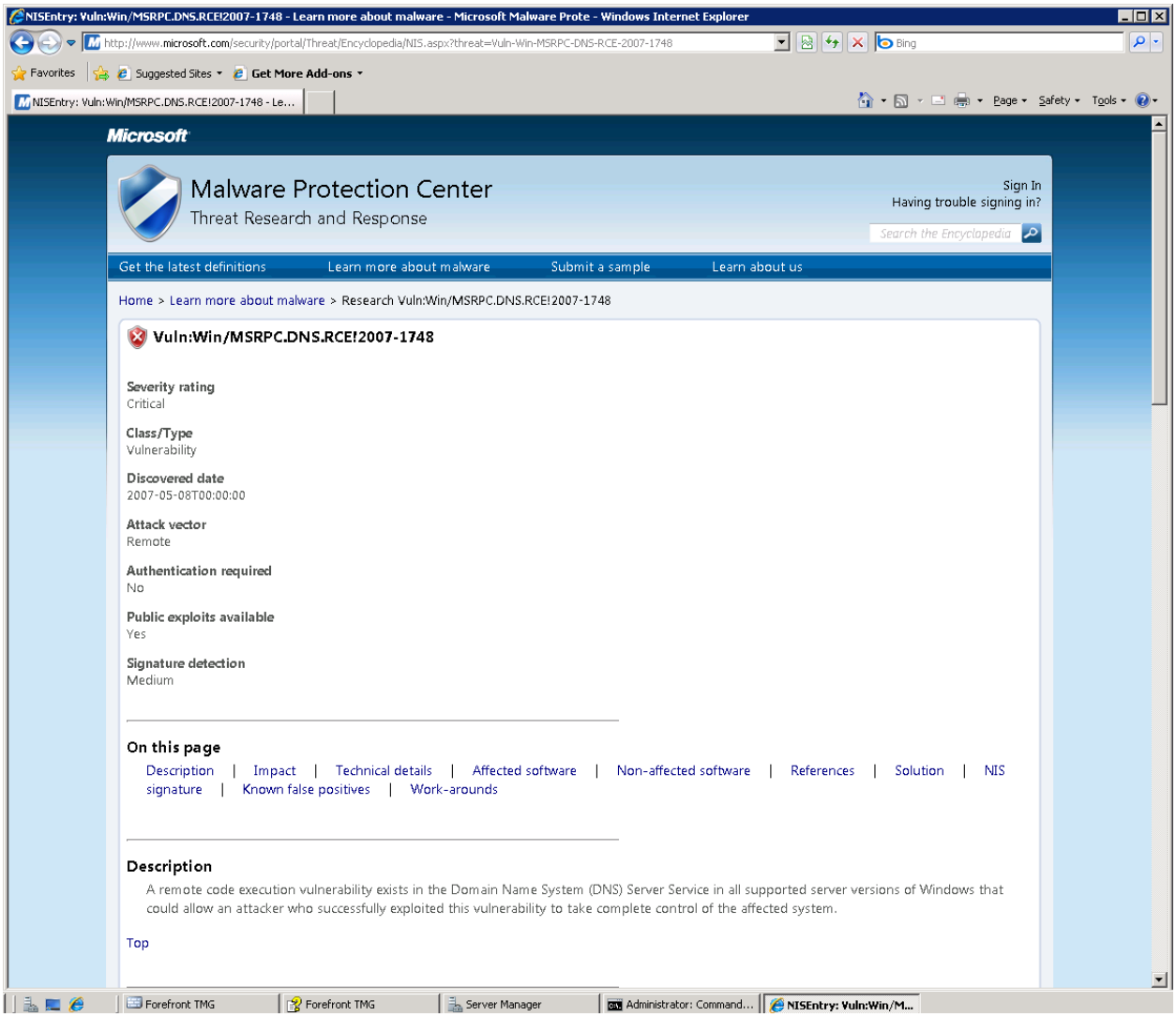


Figure 7: MMPC write up for one of NIS RPC signatures

Note that currently the search on this portal provides results only for antimalware write ups, and will not search for NIS write ups.

Deploying NIS

The following section describes how to plan a NIS deployment, how to configure it and monitor it on a Forefront TMG standalone (single server) machine. The Enterprise edition of Forefront TMG supports symmetric array configuration, including NIS configuration. The following discussed configurations are automatically applied to arrays in the Enterprise edition of Forefront TMG.

Planning NIS Deployment

Forefront TMG protects your network against exploits of known vulnerabilities in operating systems and applications using Network Inspection System (NIS). NIS is a traffic inspection system based on protocol decoding that uses signatures of known vulnerabilities to detect and potentially block attacks on network resources. When you plan to deploy NIS in your organization, note the following:

- NIS protects against network-based vulnerabilities. It does not specifically protect against file-based vulnerabilities. Malicious files and in particular, files that use exploits may also be sent over the wire. Protection against file vulnerabilities is provided by the malware inspection feature in Forefront TMG. For information, see the **Planning to protect against malicious Web content** section in the Forefront TMG help file.

- To keep your systems protected from the latest threats, verify that Forefront TMG has connectivity to the selected update source, Microsoft Update or WSUS, and that automatic installation of the latest signature set is enabled. For more information, see the Configuring Signature Updates section.

- As with any security technology, NIS consumes some computing resources while performing traffic inspection. See the Performing Capacity Planning section for details.

- When you download new signature sets from Microsoft Update, they are applied to new connections only. When you create your security policy, consider the impact on long lasting connections (such as virtual private network connections), against the security of applying the most up-to-date protection to all connections.

- NIS supports only MMPC authored and certified signatures at this time.

Deciding What Network Traffic to Inspect

Business environments may differ greatly in the variety of line of business applications they use. As a result the network protocols which are used in those environments may vary as well. The exposure of the networks to external and internal attacks varies based on the way these networks are connected to the Internet and the way Forefront TMG is deployed and configured. The administrators of the network must evaluate the risks that their environment is exposed to, and correspondingly configure security measures in order to minimize and mitigate those risks.

The recommended configuration is to enable all existing NIS signatures using their default response policy. With this configuration, NIS provides its most complete protection. However some administrators may prefer to take a more selective approach, for example to minimize the resources which are consumed during traffic inspection. Additionally, firewall best practices dictate the use of least

access traffic policies. If a protocol is not allowed by the Forefront TMG policy, NIS will not inspect that traffic. See the Forefront TMG help file for details how to configure access policy.

Using the non-default NIS signature configuration in order to control traffic inspection should be done cautiously. Protocols may be associated with other layered protocols. For example, configuring signatures for the HTTP protocol may also impact the inspection of RPC over HTTP traffic. You should enable NIS signatures for protocols which are allowed by Forefront TMG. In most workplaces, employees are permitted to browse the Internet, thus HTTP traffic should be inspected. Similarly, in order to help secure email traffic, you should let NIS inspect protocols that are used for that traffic such as SMTP, POP3, IMAP and MIME. The decision as to which protocols from this list to enable is determined by the way the email clients and the email servers are configured in the specific environment and whether Forefront TMG is configured to allow these protocols.

It is possible to enable or disable specific NIS signatures. See the Configuring Signatures Overrides section for details. Modifying specific signatures response policy may be required for trouble shooting on Internet access issues. NIS also provides an easy way for configuring all signatures for a specific protocol:

1. In the Forefront TMG Management console, in the left pane, click the **Intrusion Prevention System** node.
2. In the **Group by** drop-down list, select **Protocol**. The signatures will now be grouped by their protocol.
3. Right click on the protocol name and select the option you want to apply.

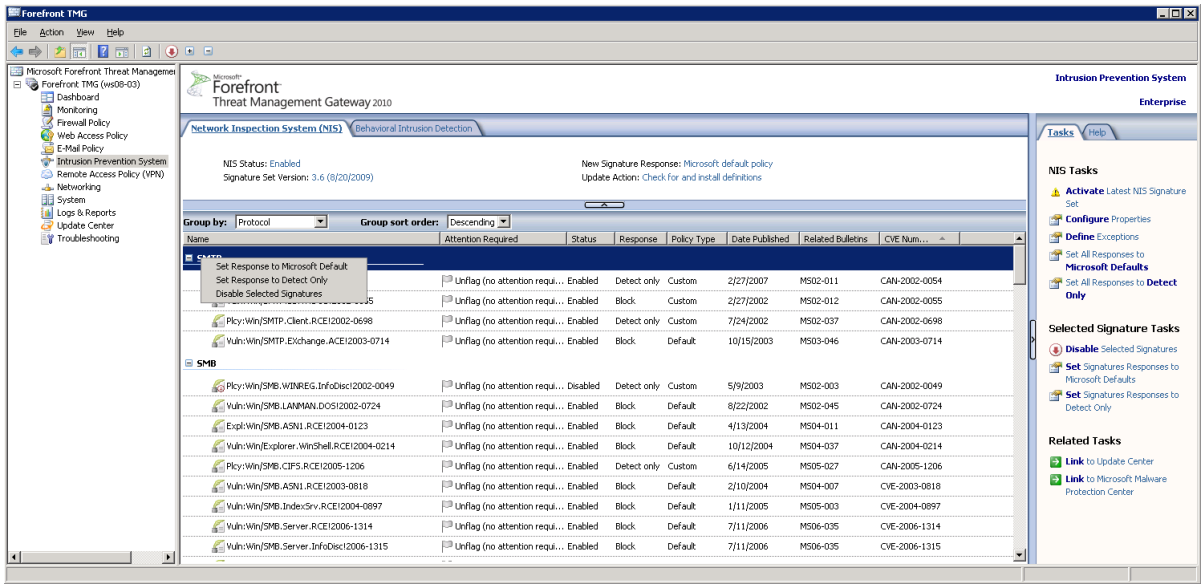


Figure 8: Grouping signatures by protocol

As a reminder, the most secure configuration would be to leave all NIS signatures enabled and configured to use their default response.

Performing Capacity Planning

NIS helps protect your organization from exploits but like any other security technology consumes some computing resources when inspecting the traffic. You should plan your hardware requirements accordingly before deploying Forefront TMG and NIS.

In a typical traffic mix, NIS adds up to 30% to the CPU load of a Forefront TMG server that also has the malware inspection enabled. The exact number can vary based on several factors such as hardware configuration, the traffic profile, the NIS configuration and additional tasks that the server performs. This estimate relies on the traffic profile described below. That profile was determined in self-host deployment at Microsoft and is likely to be different in other organizations.

Table 1: Protocol traffic profile used for estimating the CPU load

Protocol	HTTP	SIP	FTP	DNS	SMTP
Percent of the traffic	80%	8%	5%	5%	2%

Considering this estimate, you should adjust your CPU requirements when planning to enable NIS. The exact requirement depends on characteristics that are specific to the environment and the traffic profile served by your Forefront TMG deployment.

Configuring NIS

The following section describes how to enable and configure NIS in Forefront TMG. The Forefront TMG Getting Started Wizard simplifies the steps to enable NIS and configure signatures updates and telemetry reporting. By default, all NIS signatures use the response defined by the MMPC response team. However NIS also provides granular signature configuration. For example, you can:

- Use older signature sets for troubleshooting.
- Configure specific signatures to allow traffic and log an event.
- Define exceptions for traffic inspection.
- Enable the Protocol Anomalies detection feature.

Enabling NIS

When you enable NIS, Forefront TMG can help detect and block exploit attempts, so systems which are not fully updated are still protected against many attacks from the Internet. If configured to do so, NIS receives periodic updates from Microsoft Update to protect against recently discovered vulnerabilities and exploits. In order to allow NIS to begin traffic analysis, you have to enable it and configure it to receive the latest NIS signatures. Follow these steps to enable NIS on your Forefront TMG and keep it up to date:

1. In the Forefront TMG management console, click the **Forefront TMG < *name*>** node.
2. On the **Tasks** tab, click **Launch Getting Started Wizard**.

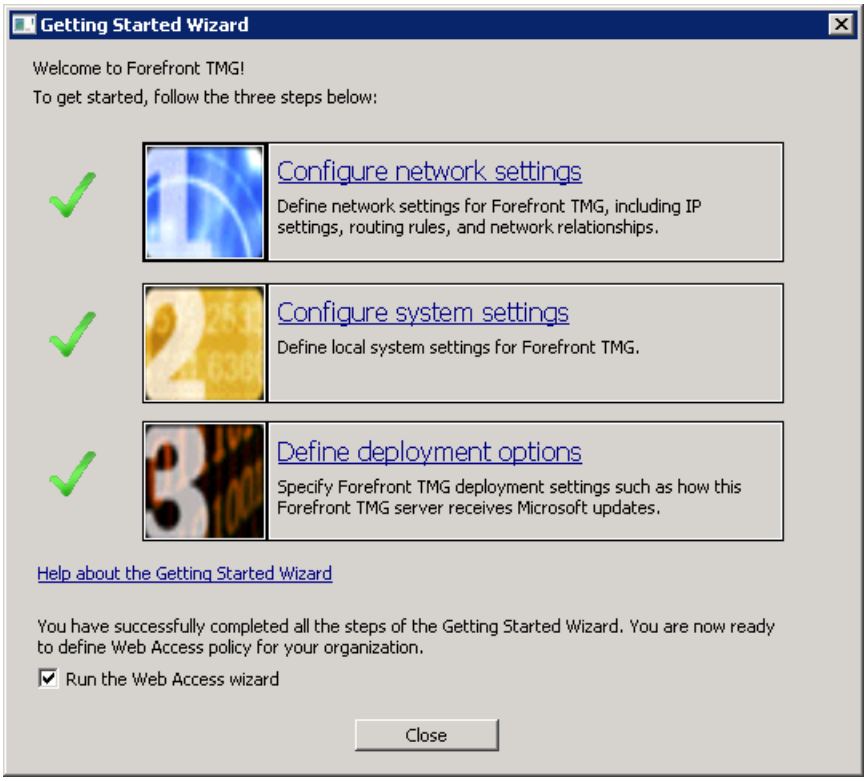


Figure 9: Forefront TMG Server Getting Started Wizard

3. Click **Define deployment options** and click **Next**.
4. On the **Microsoft Update Setup** page, verify that **Use the Microsoft Update service to check for updates (recommended)** is selected in order to receive the latest updates. This option applies even if you use WSUS to obtain updates. For more details on how to configure Forefront TMG to receive updates from a WSUS server, see the "Managing definitions updates for Forefront TMG" page in Forefront TMG help fie. Click **Next**.

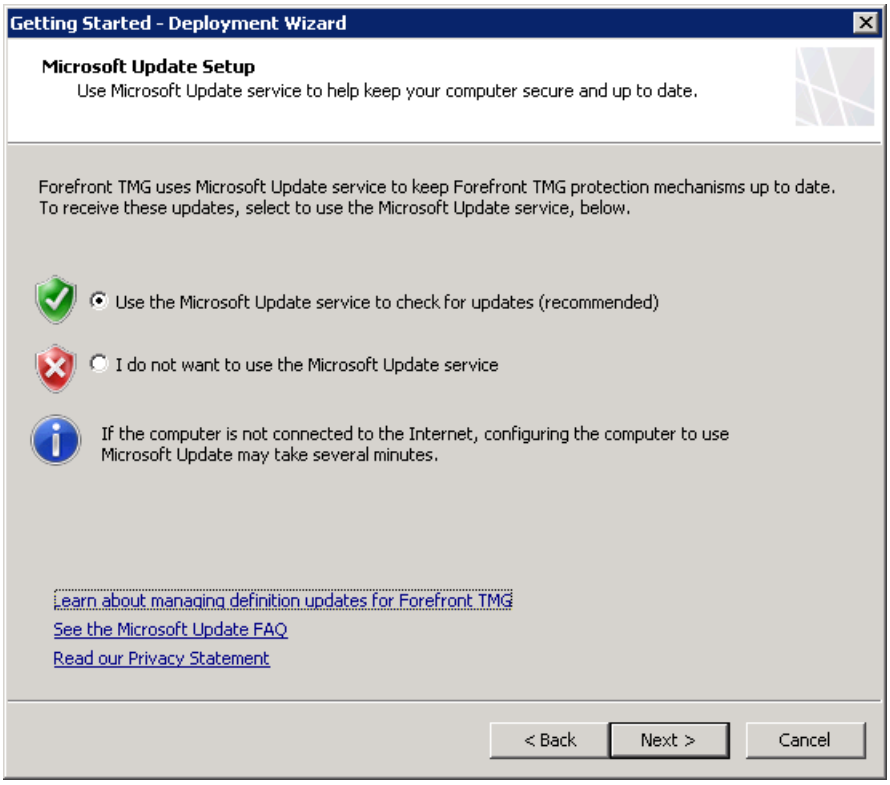


Figure 10: The Microsoft Update Setup page in the Forefront TMG Getting Started Wizard

5. On the **Forefront TMG Protection Features Settings** page, verify that the license for NIS is set to **Activate complementary license and enable NIS**.

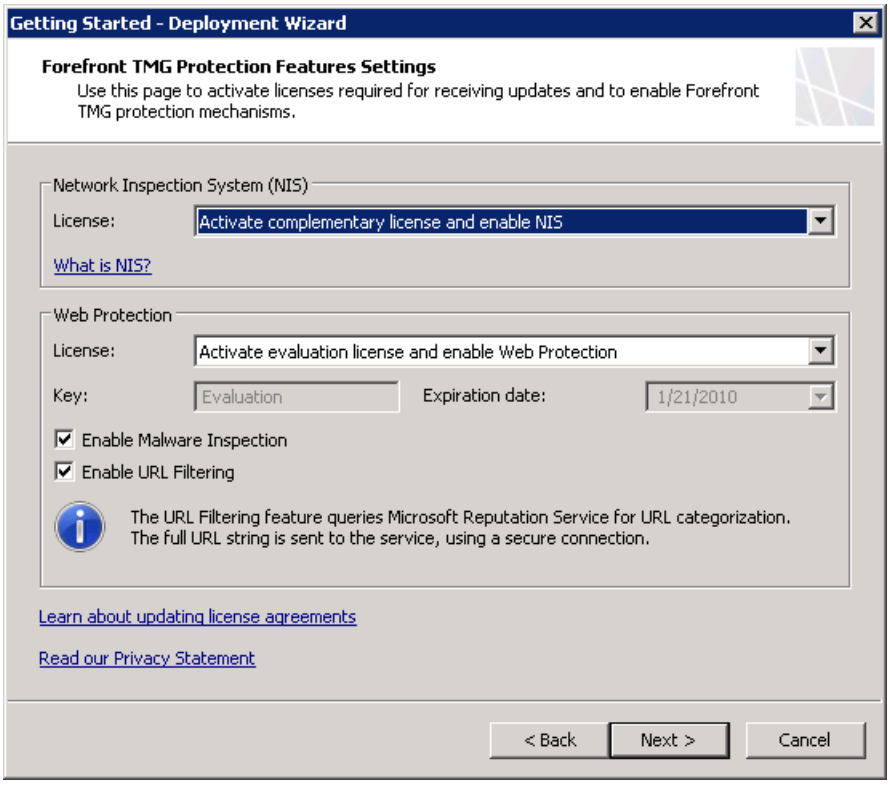


Figure 11: The Protection Features Settings page in the Forefront TMG Getting Started Wizard

6. On the **NIS Signature Update Settings** page:
    1. If you want to automatically install new signature sets, ensure that **Check for and install definitions (recommended)** is selected.

    2. The **Automatic polling frequency** setting applies to NIS only. The polling frequency settings for other updatable protections are located in the **Update Center**.

    3. The **response policy for new signatures** setting applies only to newly downloaded and installed signatures. You should set it to **Microsoft default policy (recommended)**. If you select a different response policy, new signatures will be flagged for attention on the **Network Inspection System** tab.

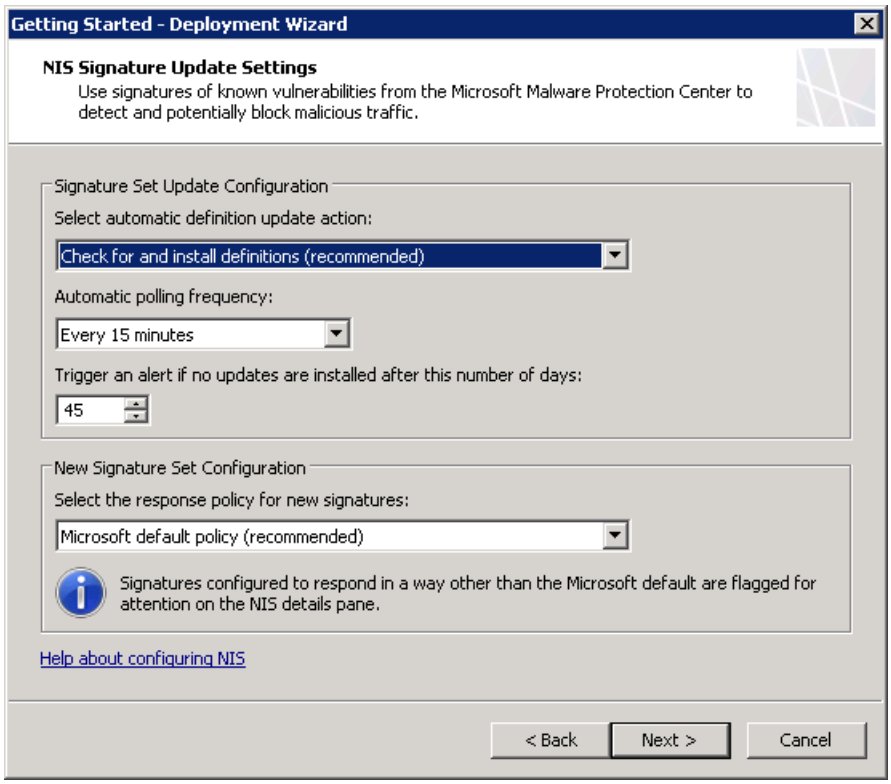
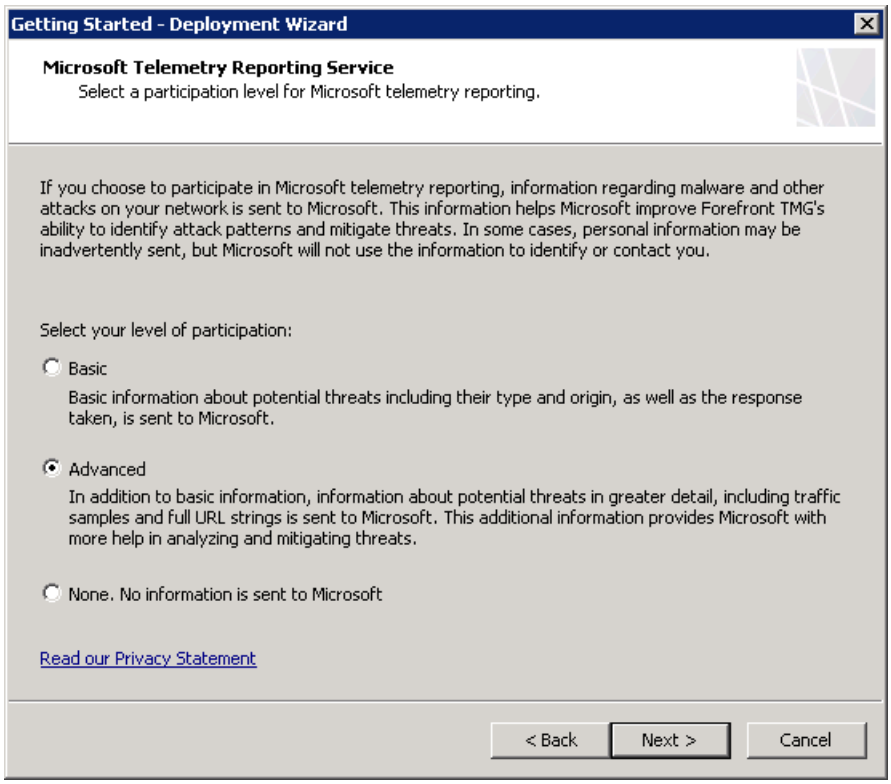


Figure 12: The NIS Signature Update Settings page in the Deployment Getting Started Wizard

4. In the **Microsoft Telemetry Reporting Service** page, select your preferred participation level. Please see the Telemetry Service section for more details about the telemetry and the Understanding the Research and Response for NIS section for details how telemetry helps the Microsoft research and response process.



5. Complete the wizard and click **Finish**.

Now NIS is enabled and functional. No additional configuration is required.

Configuring Signature Updates

This section describes how to configure automatic signature updates for NIS in Forefront TMG. NIS uses signatures developed by the MMPC to protect unpatched systems from attacks that exploit known vulnerabilities of Microsoft products. To keep your systems protected from the latest threats, you should verify connectivity to Microsoft Update service and enable automatic installation of the latest signatures.

Before you can use Forefront TMG to block exploit attempts against known vulnerabilities, you must first download the latest NIS signature set. Follow the instructions below to configure NIS signature set updates.

To manage NIS signature set downloads:

1. In the Forefront TMG Management console, click the **Intrusion Prevention System** node.
2. On the **Tasks** tab under **NIS Tasks**, click **Configure Properties**.
3. On the **Definition Updates** tab, under **Automatic definition update action**, select one of the following options:
    - **Check for and install definitions (recommended)** - select this option to automatically download and install the latest signature updates.

- **Only check for definitions** - select this option to be notified of new signature sets but not to automatically download or install them.

- **No Automatic action** - select this option to disable automatic updates.

4. Under **Response policy for new signatures**, select one of the following options:
   - **Microsoft default policy (recommended)** - select this configuration to use the default response policy defined by the MMPC for each signature.

   - **Detect only response** - select this option to log but not block traffic matching any new signature.

   - **No response (disable signature)** - select this option to take no action on signature matches.

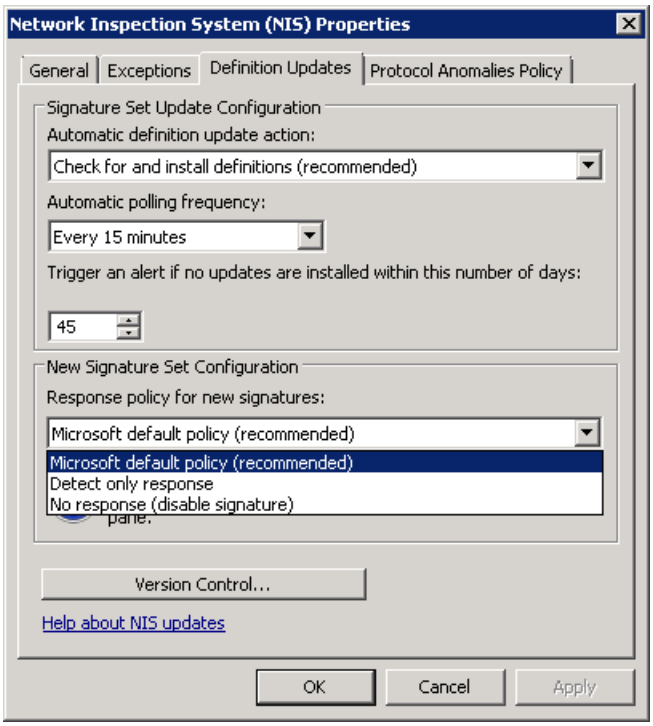


Figure 13: The Response Policy setting for new signatures

Verifying that NIS is Receiving Updates

Follow these steps to make sure that NIS is receiving signature updates:

1. In the Forefront TMG Management console, in the left pane, click **Update Center**.
2. In the details pane, make sure that the **Last Update Status** for the NIS entry shows **Up to date**.
3. If not, click **Check for Definitions** in the **Definitions Updates Tasks** list on the right.

The NIS entry shows the signature version and when it was last updated:

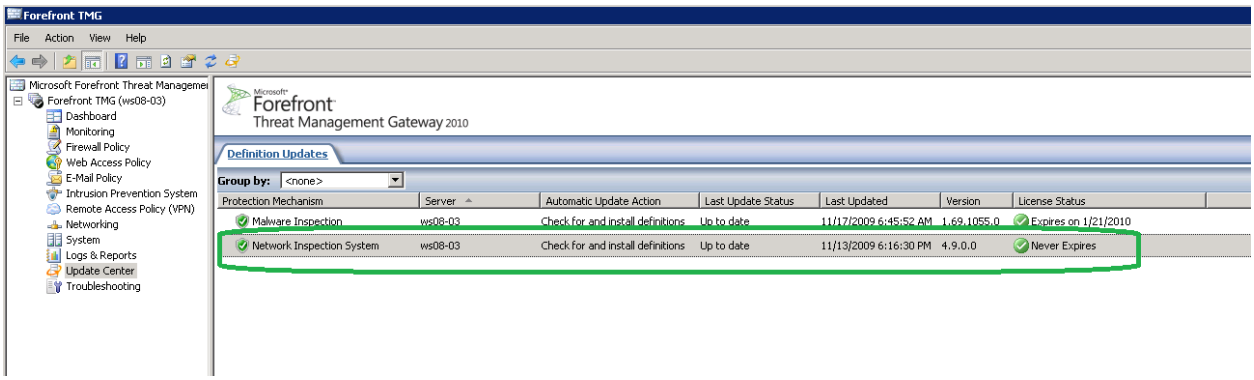


Figure 14: The NIS update details in the Forefront TMG Update Center

You can also find these details in the details pane for NIS. See the Granular Configuration section below for details.

If the system fails to download updates, see the Signature Set Updates Failure section.

Selecting an Older Signature Set

In some cases, you may want to temporarily use an older signature set, for example to troubleshoot incidents of blocked traffic. NIS provides you the ability to use any signature set which is locally available.

1. In the Forefront TMG Management console, click the **Intrusion Prevention System** node.
2. On the **Tasks** tab under **NIS Tasks**, click **Configure Properties**.
3. On the **Definition Updates** tab, click **Version Control…**
4. A **Signature Set Version Control** page will open. Check the **Select the NIS signature set you want to activate** option.
5. Select the signature set you would like to activate from the drop down list.
6. Click **Activate** and then Click **OK**
7. Click **Apply** on the apply changes bar.

When you activate an older signature set, NIS will not use signatures from newer signature sets. Therefore this configuration involves some risk. Configure NIS to use the latest signature once the need for the older signature set is resolved. . NIS will trigger an alert every time a new signature set becomes available while it is configured to use an older signature set. Also a task to **Activate the Latest NIS Signature Set** will be added to the NIS Tasks menu:

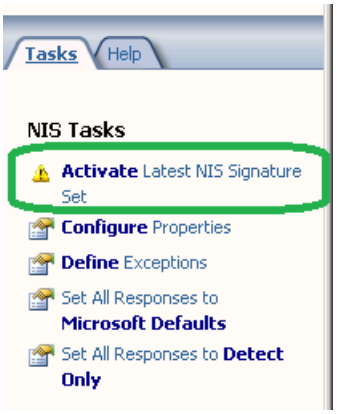


Figure 15: The Activate Latest NIS Signature Set option

Granular Configuration

NIS provides you granular control over policy configuration. NIS signatures are released with a predefined recommended policy. The MMPC has set the recommended policy based on multiple factors including the vulnerability severity, business impact, current incidents and others. The MMPC team may change the recommended policy automatically through signature updates. The administrators may choose to use their own policy, such as setting a signature to detect only instead of block and that custom policy will be preserved even with future NIS signature sets.

The high level configuration of NIS is presented at the top of the **Network Inspection System (NIS)** tab after you select the **Intrusion Prevention System** node in the left pane.

The following settings are displayed in that area:

- NIS status
- The signature response policy
- The version of the active signature set
- The update action (whether to check and/or install new definitions)

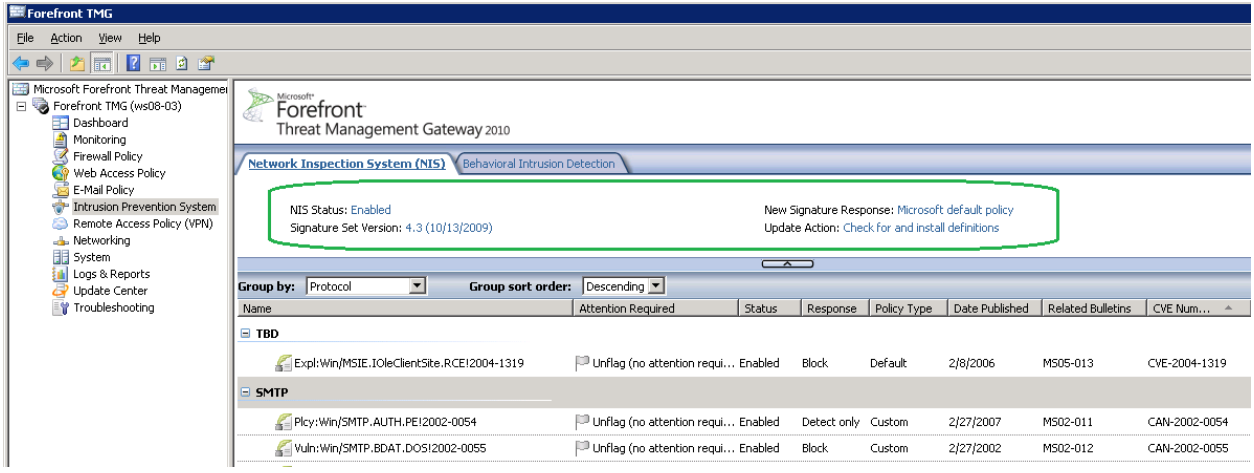


Figure 16: The NIS tab in Forefront TMG management console

Using NIS Tasks

When you click the **Intrusion Prevention System** node in the left pane, the **NIS Tasks** tab will show in the right pane:

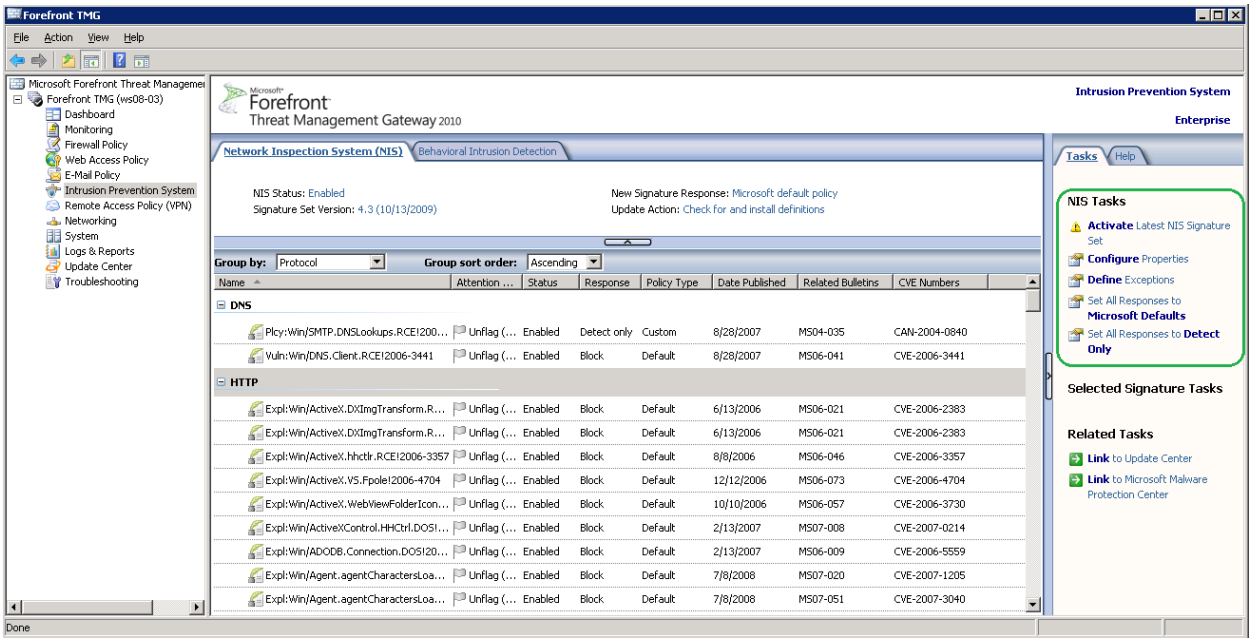


Figure 17: The NIS Tasks menu in Forefront TMG management console

Here is a closer look at this menu:

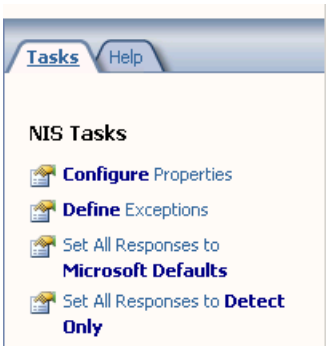


Figure 18: NIS Tasks menu

Selecting **Configure Properties** opens the main **Network Inspection System (NIS) Properties** page.

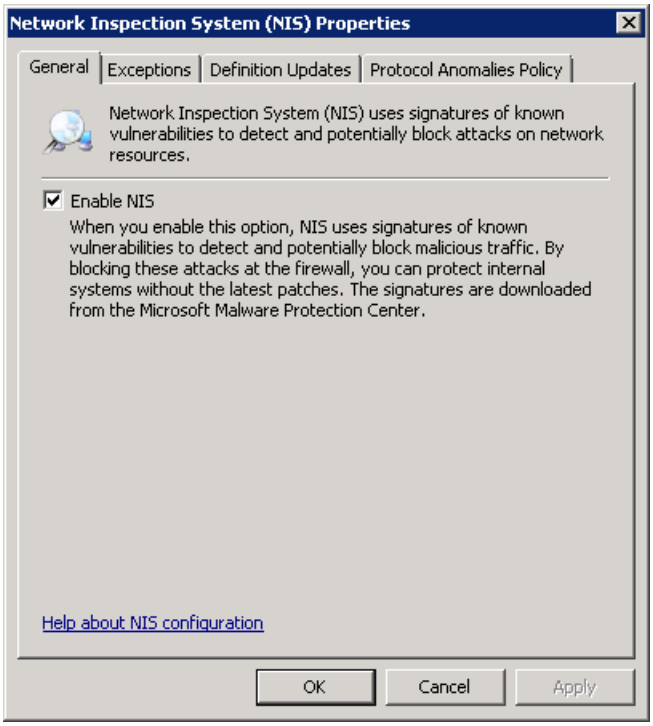


Figure 19: The General tab for NIS Properties configuration

You can choose whether to enable or disable NIS. If you choose to disable NIS, your policy configuration (signature overrides, new signature policy, exception list etc.) are retained. Once you re-enable NIS, it will use the previous configuration.

Configuring Exceptions

NIS allows you to exclude certain network entities from network inspection. You may choose to exclude specific traffic for capacity adjustments or as part of troubleshooting. Forefront TMG allows adding exceptions using the following network entities:

- Networks: Several predefined networks are provided such as the external network, the internal network and the local host.
- Network sets: These entities include groups of networks. Several predefined groups are provided and a wizard is available to create new network sets.
- Computers: Computers are specified by their IP address.
- Computer sets: Several predefined sets are provided. It is possible to define new computer sets by specifying the computers, IP address ranges or subnets.
- Address ranges: It is possible to define new address ranges.
- Subnets: It is possible to define new subnets using the network address and network mask.
- Domain name sets: Numerous predefined sets are provided such as Microsoft Updates sites. It is also possible to define new sets by adding list of domain names.

NIS will not scan traffic to or from a network entity that is included in the exception list.

Exceptions that use domain name sets are applied only to HTTP traffic that is sent to these domains.

To manage NIS exceptions, follow these steps:

1. In the Forefront TMG Management console, in the left pane, click the **Intrusion Prevention System** node.
2. On the **Tasks** tab under **NIS Tasks**, click **Define Exceptions**.
3. On the **Exceptions** tab, click **Add…**, and select the network entities you want to exclude from inspection.
4. Click **OK**.
5. Click **Apply** on the apply changes bar.

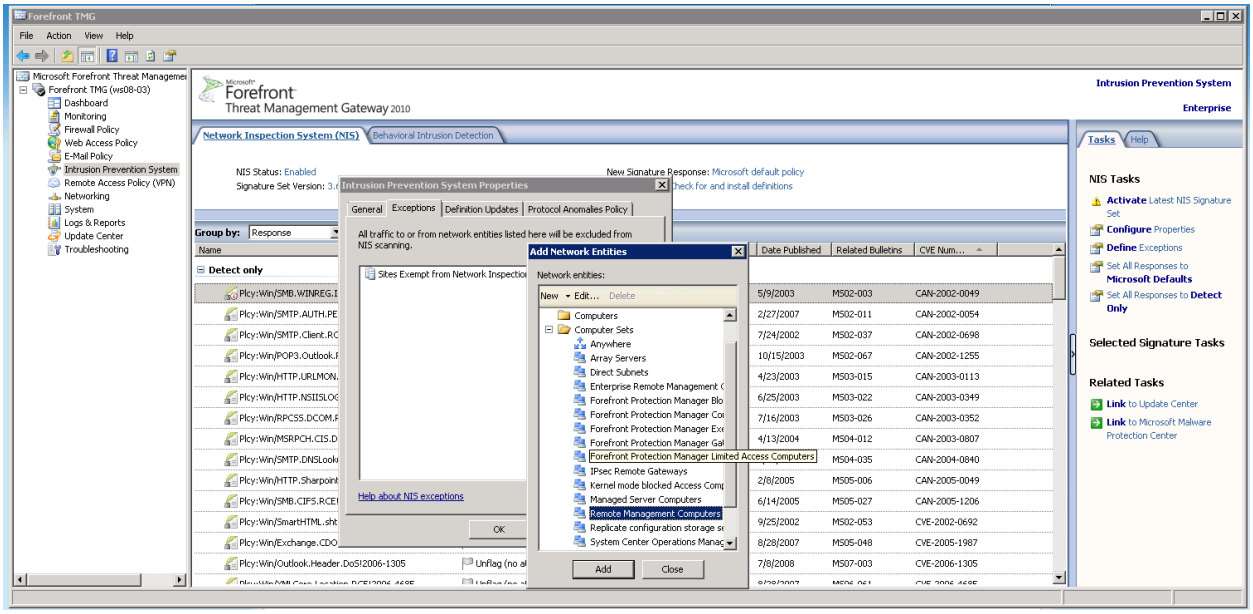


Figure 20: Configuring NIS exceptions

Configuring Protocol Anomalies Policy

NIS offers a unique feature to tighten your organization's security by detecting and blocking anomalies in network traffic. The protocol anomaly detection functionality looks for cases where the network traffic is not in compliance with protocol standards such as RFCs and common implementations.

Protocol implementations may differ from RFCs and from one another. In some cases this is by design and serves a legitimate purpose. In other cases, protocol anomaly detection may alert on a network attack designed to evade intrusion prevention systems. By configuring NIS to block protocol anomalies, you will be alerted when those cases happen and you can further investigate their potential malicious intent. Note that blocking such traffic may cause valid applications to fail.

Using telemetry, MMPC is constantly enhancing the NIS protocol definitions to understand legitimate traffic as observed in production deployments. When new protocol definition updates are available, they are delivered with a new NIS signature set.

To configure Protocol Anomalies Policy:

1. In the Forefront TMG Management console, click the **Intrusion Prevention System** node.
2. On the **Tasks** tab under **NIS Tasks**, click **Configure Properties**.
3. On the **Protocol Anomalies Policy** tab, under **Response to protocol anomalies**, select one of the following options:
    - **Allow**, to avoid blocking legitimate traffic, or
    - **Block**, to tighten security.

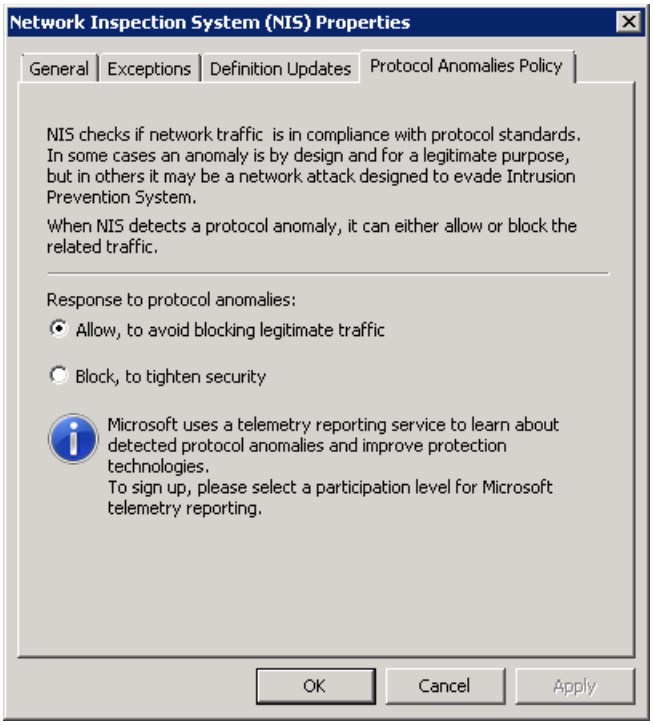
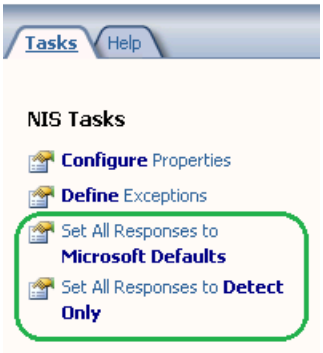


Figure 21: NIS Protocol Anomalies Policy tab

Protocol Anomalies policy is set by default to **allow** traffic when protocol anomalies are detected. In this mode, protocols anomalies are not alerted or logged. If the protocol anomalies policy is configured to **block,** NIS blocks the traffic when protocol anomalies are detected and triggers a TMG alert. TMG includes NIS detection information in the traffic log to assist with potential troubleshooting. See the Troubleshooting NIS section for examples of a log entry and an alert for protocol anomaly detection.

Configuring Global Response Policy Setting

Fundamentally, NIS can operate as an IPS or as an IDS system because NIS signatures can be configured to either block or detect (log) malicious traffic. An administrator may want to configure NIS to only detect but not block malicious traffic as part of testing; however NIS does not provide actual protection under such configuration. You should change the response to Microsoft default response, as soon as the testing is complete. To configure the global response policy, select the appropriate **Set All Responses** option from the **NIS Tasks** menu:



This will open the **Global Response Policy Setting** page with the corresponding setting selected:

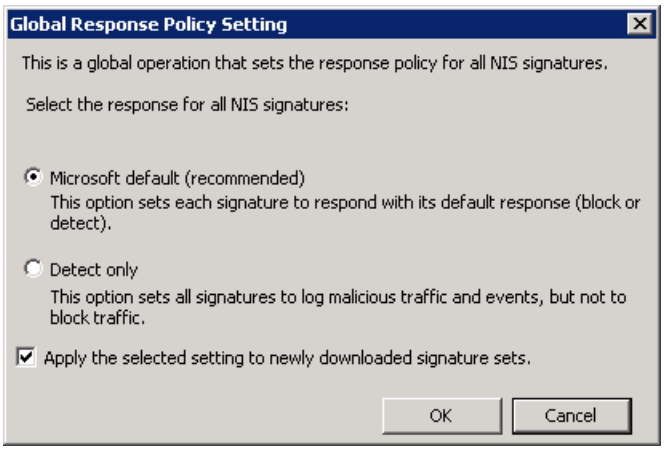


Figure 22: The Global Response Policy Setting page

You can also configure whether the block or detect setting be applied to newly downloaded signature sets. This option is enabled by default.

Configuring Signatures Overrides

NIS allows you granular control over policy configuration on a signature level. Each signature is released with a recommended response policy as set by the MMPC. You are able to define your own policy for each signature, for example by configuring the signature to only detect certain traffic but not to block it. Future signature updates will not change these settings.

You can change policy for a specific signature or for multiple selected signatures. To change the setting for a specific signature, simply select it and use the options which are available in its right-click menu. Or you can double-click on that signature, and make the change in the properties page for that signature. You can configure whether to use the Microsoft default response for that signature, or to override it.

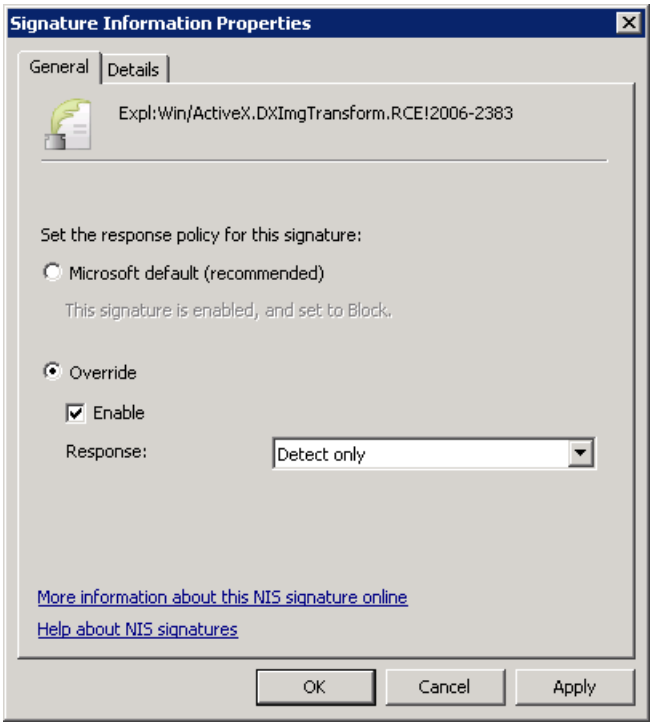


Figure 23: A Signature Information Properties page

To select a group of signatures, you should group the signatures by choosing one of the options from the **Group by** pull down available in the NIS tab: **Attention Required**, **Response**, **Policy Type**, **Business Impact**, **Category**, **Date Published**, **Severity**, **Fidelity**, **Protocol** or **Status**.

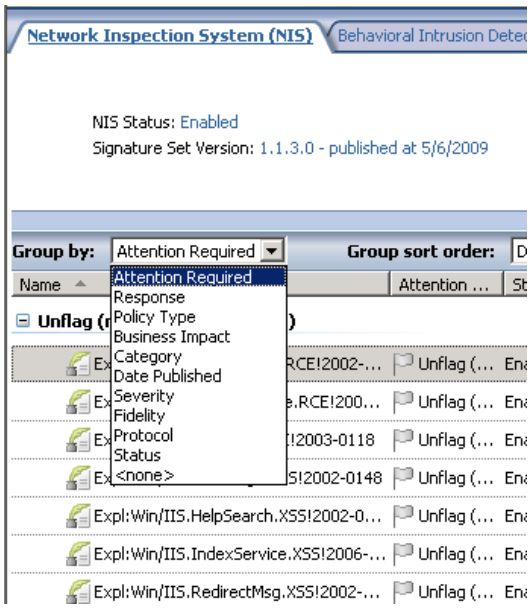


Figure 24: The signatures Group By drop down list

Once a group of signatures is selected, you can choose the appropriate policy from **Selected Signatures Tasks** in the **Task Menu tab**:

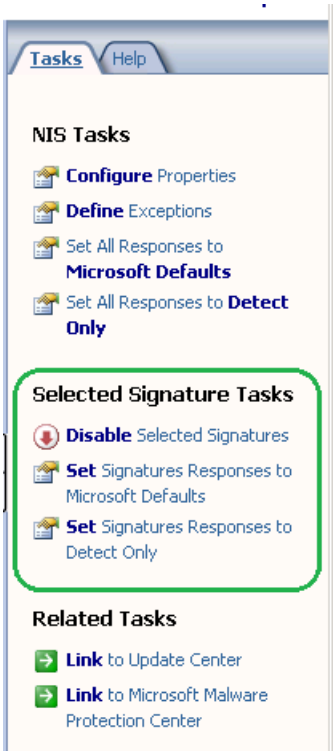


Figure 25: The Selected Signature Tasks menu

You can also right click to select an option for the chosen group:

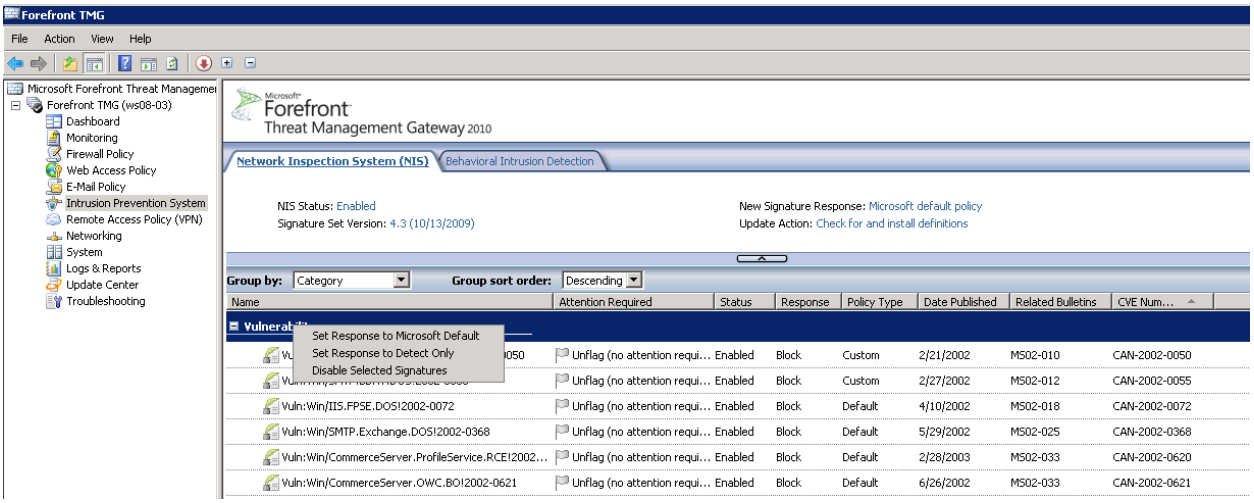


Figure 26: Options for a selected group of signatures

Configuring Telemetry

Forefront TMG can be configured to send telemetry to Microsoft. The Telemetry Service and Understanding the Research and Response for NIS sections provide more information on how telemetry helps the MMPC analyze and respond to emerging threats. You can modify or cancel your Microsoft Telemetry Service membership at any time. To do that:

1. Select **Properties** from the right-click menu of the Forefront TMG server in the left pane.
2. Select the **Telemetry Reporting Service** tab
3. Select the desired level of participation

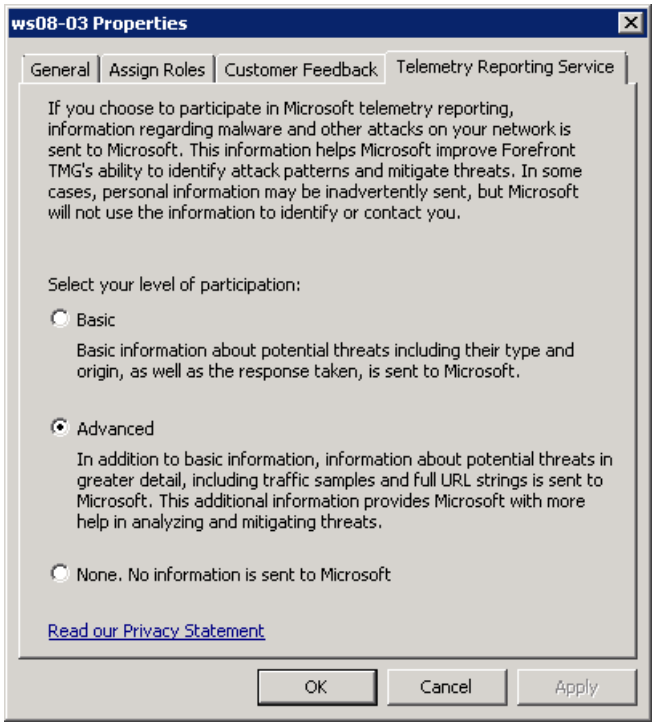


Figure 27: The Telemetry Reporting Service page

The link at the bottom of the page points to the Forefront TMG online privacy statement

Testing NIS Deployment

You don't have to wait for a real attack to see NIS in action. NIS is released with a few test signatures which can be triggered by specific traffic. You are encouraged to try these test signatures, since they help verify NIS behavior, as well as simulate user and administrator detection experience.

Testing with the HTTP test signature

The HTTP test signature allows you to test how NIS blocks malicious HTTP traffic. You can find the HTTP test signature in the Forefront TMG management console:

1. Select the **Intrusion Prevention System** node in the left pane
2. Find the **Test:Win/NIS.HTTP.Signature!0000-0000.** Grouping signatures by protocol or by category simplifies this task:

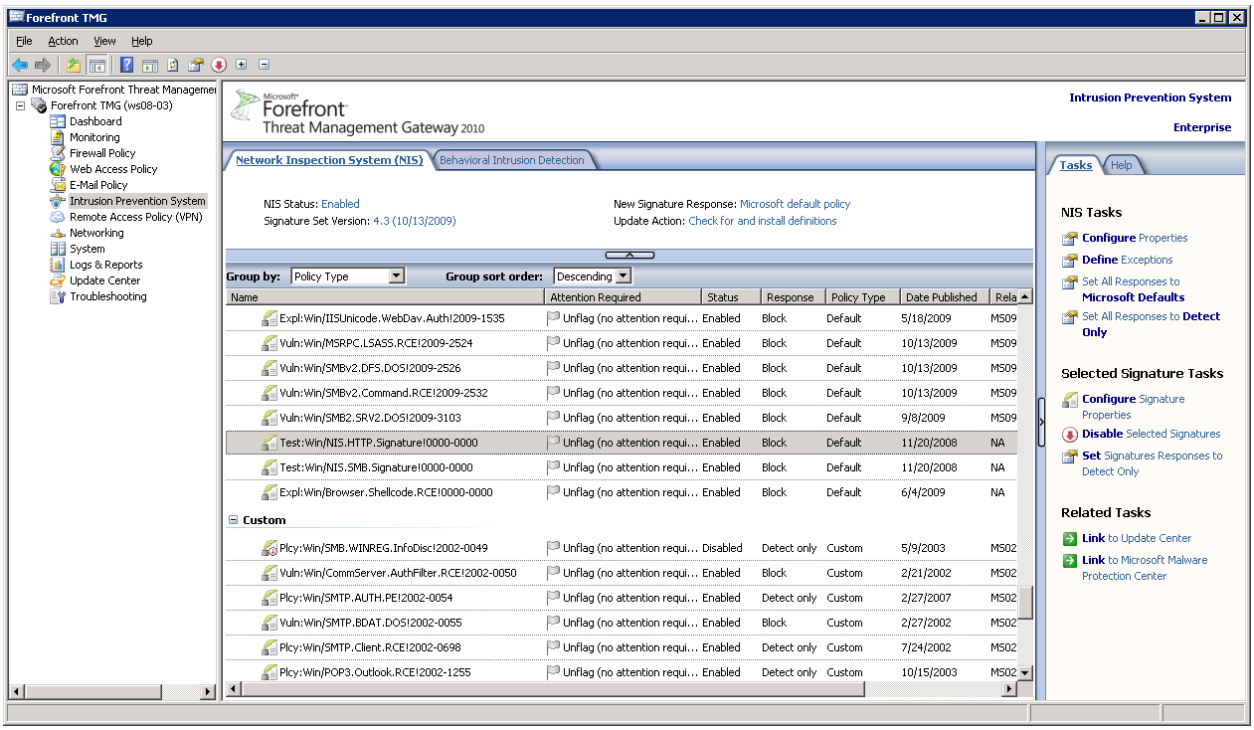


Figure 28: The NIS HTTP test signature

During HTTP traffic inspection, the host header, path, and query string are extracted from the request. NIS compares the host header and the query string to the test signature. If they match, detection occurs. If the signature response is "Block", Forefront TMG will send the error response page back to the client and close the connection.

Though the test signature is quite simple, a similar process applies to other protocols inspected by NIS, among them DNS, RPC, SMB and email protocols.

Here's how to verify the *status* and *response* of the HTTP test signature. The signature has to be enabled and its response configured to block. Double-clicking the signature open its properties page:

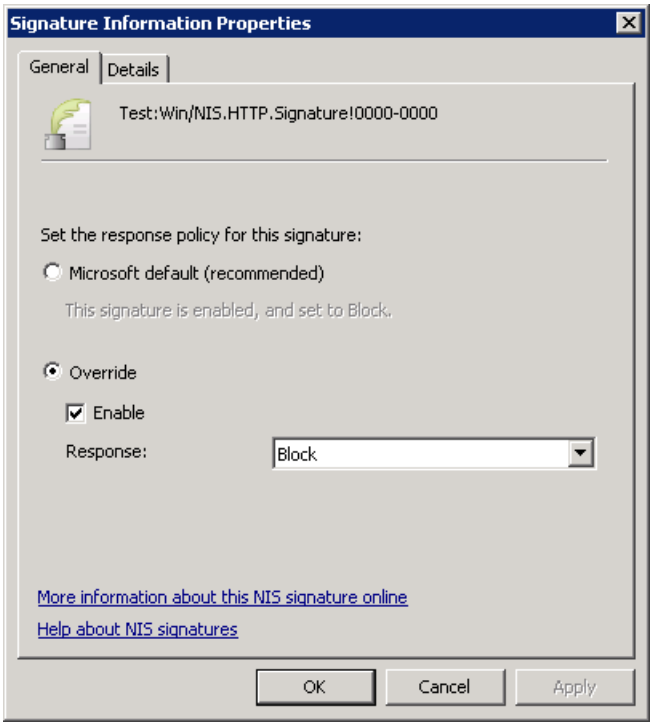


Figure 29: The properties page for the HTTP test signature

In order to trigger the test signature, you'll need to use a specific URL in a Web browser from a computer that is connected to the Internet through the Forefront TMG server. You can send the request either as a SecureNAT, TMG Client or Web proxy client. The URL is http://www.contoso.com/testNIS.aspx?testValue=1!2@34$5%6^[{NIS-Test-URL}]1!2@34$5%6^. It is also provided in the write up for this NIS test signature. Follow the "More information about this NIS signature online" link at the bottom of the properties page.

Copy and paste the URL to the address bar of the browser and click enter:

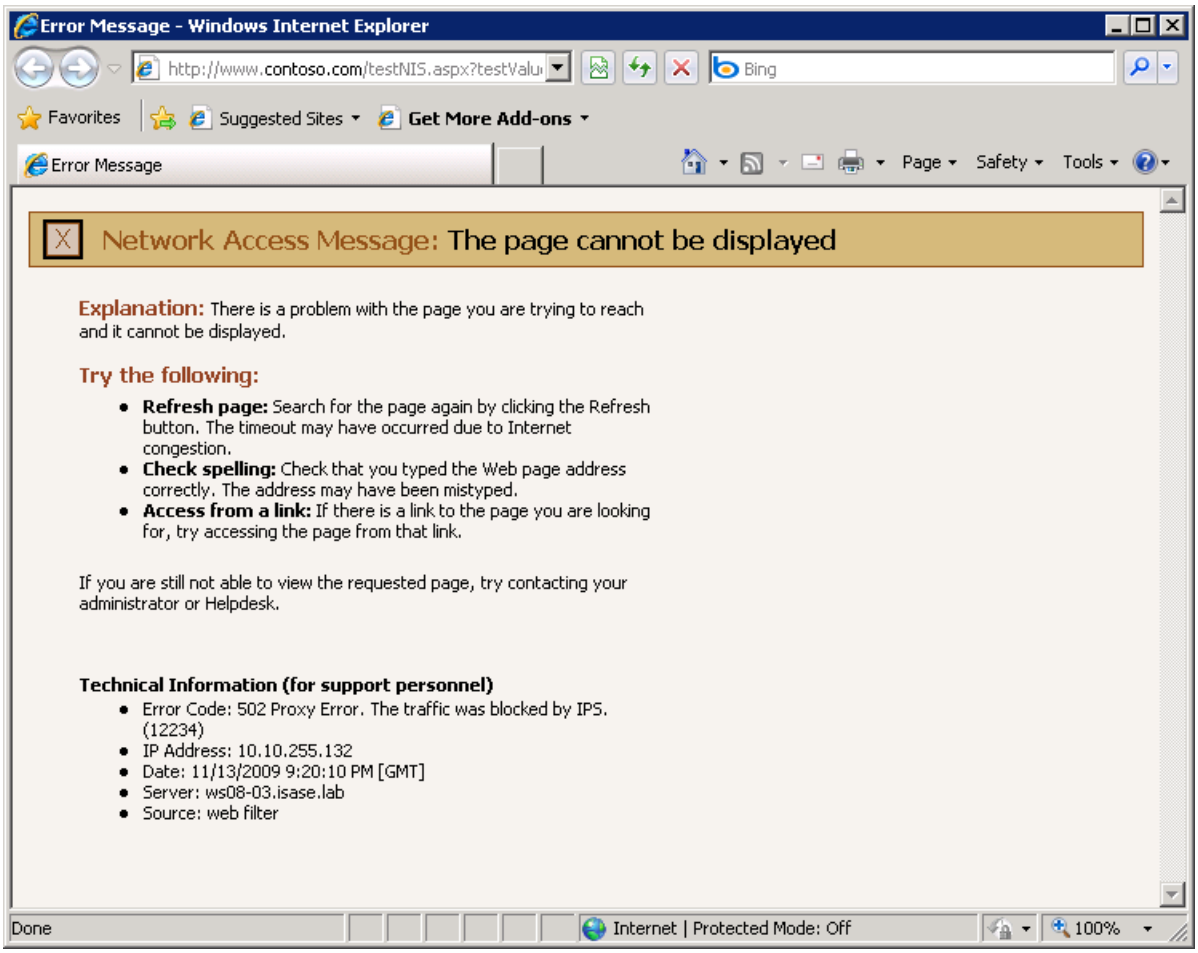


Figure 30: Blocked access with the HTTP test signature

The attempt is blocked by NIS as indicated by the secondary error code (12234) in the error page. That's the expected behavior for this test. If it doesn't work as expected (the access attempt is not blocked), the most common reasons are:

1. The URL in the address bar is incorrect.
2. NIS is not enabled. See the Configuring NIS section for details how to enable it.
3. The test signature is not enabled
4. The test signature is not configured to block.
5. The HTTP request is not sent through the Forefront TMG server.
6. This traffic is excluded from inspection by a NIS exception. See the Configuring Exceptions section for details.

The incident is logged by Forefront TMG:

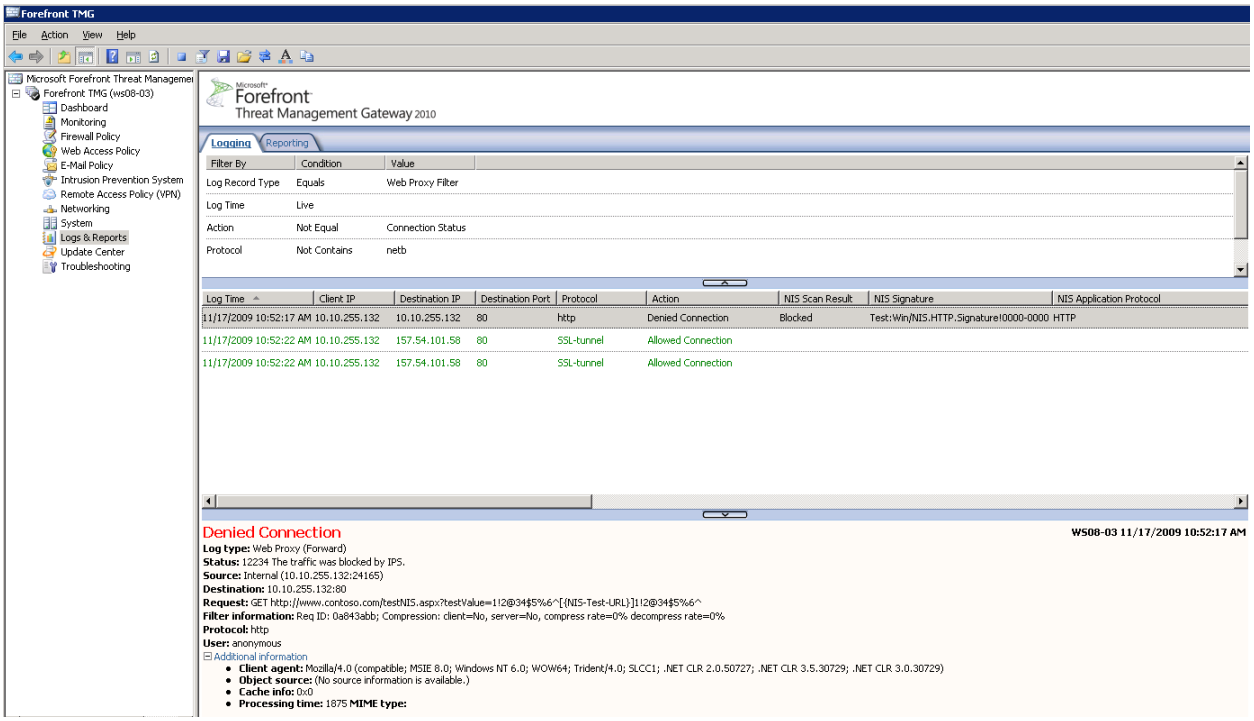


Figure 31: The log entry for the blocking of the HTTP test signature

Note that if the Log Time in the logging filter is set to Live (as shown above), you need to start the query and then access that URL. If you have already made the access attempt, and now want to see the log for that event, change the Log Time to use one of the past values such as Last Hour.

Forefront TMG also raises an alert when the traffic is blocked:

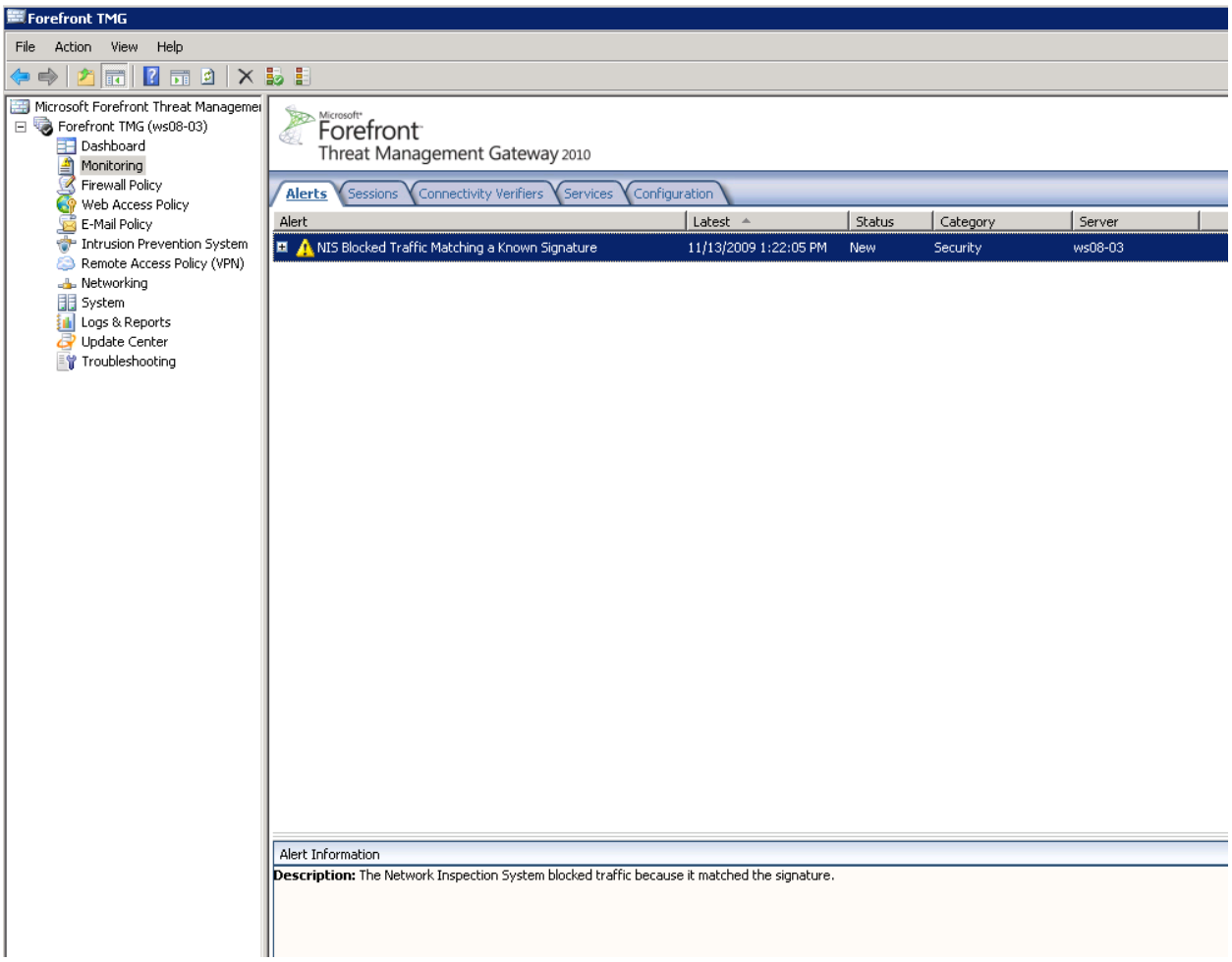


Figure 32: Forefront TMG alert for traffic blocked by NIS

Testing with the SMB test signature

NIS includes a test signature that detects specific traffic over SMB, a network protocol commonly used to access file shares. SMB traffic may be seen when Forefront TMG is installed within the network (Site-To-Site scenario) or when a VPN client connects to the network through Forefront TMG.

The name of the signature is **Test:Win/NIS.SMB.Signature!0000-0000**. In order to trigger it, copy a file with the name C0AABD79-351B-4c98-8AE7-69F4279FEF54.txt to a remote share through Forefront TMG. If the signature is enabled and configured to block, that copy action will be blocked. For more details, see the online encyclopedia entry for this signature at: http://www.microsoft.com/security/portal/Threat/Encyclopedia/NIS.aspx?threat=Test-Win-NIS-SMB-Signature-0000-0000. As with the HTTP test signature discussion above, TMG will trigger an alert and log the traffic details.

Monitoring NIS

The following section provides details how to monitor NIS.

Monitoring NIS Signatures

NIS offers manual and automatic flagging of specific NIS signatures in the Forefront TMG management console for future reference. Similar to the “important” or “unread” flags in email clients, NIS flags specific signatures for administrator attention.

Manual Flagging for Attention

You can manually flag any signature or group of signatures for future reference for example after changing a signature’s default settings. To do this, right click the signature and choose ***Flag for Attention.***

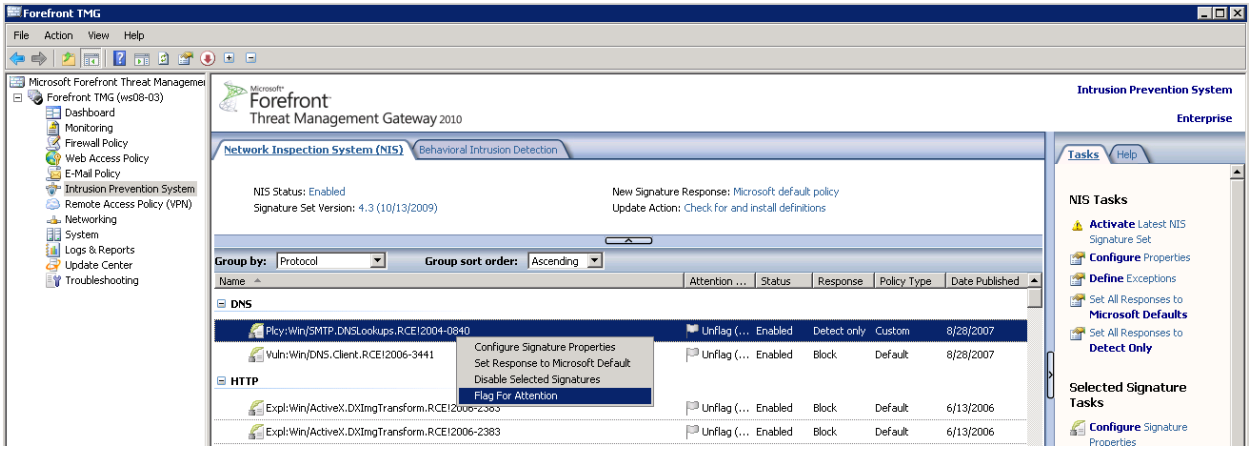


Figure 33: Flagging a signature for attention

You can provide comments in the signature properties page Details tab:

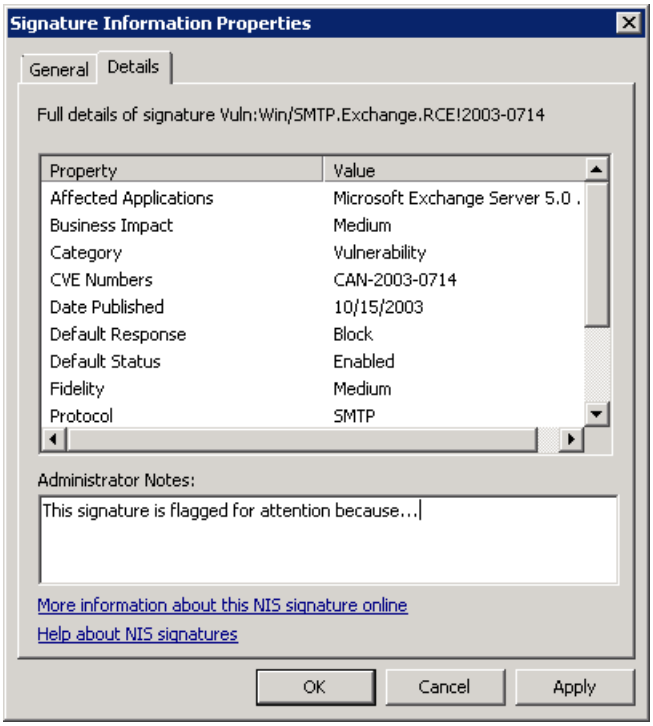


Figure 34: Adding Administrator Notes for a NIS signature

You can un-flag signatures at any time by using the **Unflag (No Attention Required)** option from their right-click menu.

Automatic Flagging for Attention

NIS will automatically flag new signatures for your attention when the global response policy for new signatures is *not* set to Microsoft default. See the **Configuring Signature Updates** section for details. The flagging helps you identify the new signatures and take appropriate action.

Using Automatic Flagging for Staging

The automatic flagging can be a useful feature to test new signatures before fully deploying them. In that case, change the global response policy to detect only (or no response). When a new signature arrives, NIS will flag all the new signatures for you automatically. You can now group the signatures by the Attention Required, and review the list of flagged signatures.

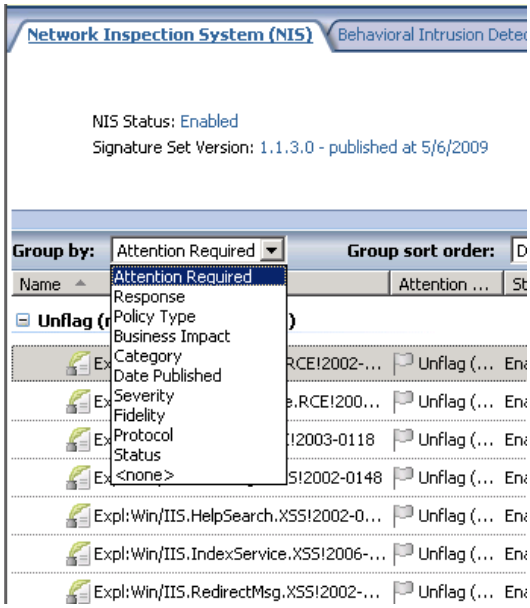


Figure 35: Grouping signatures that are flagged for attention

Once the staging testing is complete, you can change the flagged signatures to Microsoft default response. Once you are done, no signatures are flagged for attention. You can repeat this process every time new signatures are released and therefore flagged for attention. Note that during this process, due to the change in the response policy for new signatures, you won't have the protection as early as the signature release time.

Automatic Flagging of Signatures with Overridden Policy

If you override the response policy for specific signatures, for instance, by setting a "Block" signature to "Detect only", NIS will not automatically change the response if the signature response is updated by MMPC. However NIS will flag that signature for attention. For example, if you change the response for some Moderate severity signature from the default value to "Detect only", this signature will be flagged if the MMPC raises the signature severity to Critical due to changes in the threat landscape. Under these circumstances, you might want to consider changing this signature to Microsoft default. The flagging helps draw your attention to changes to the signature.

Once you override a signature default policy you must manually set it back to Microsoft default to allow for dynamic response policy setting by MMPC.

Monitoring NIS Performance

Performance counters useful to get live data from computer services and products, in order to monitor their health or capture information for troubleshooting. NIS provides the following performance counters:

Table 2: NIS performance counters

Counter group name	Counter name	Description

Forefront TMG Firewall Service:		
	Connections Blocked by NIS	The number of connections blocked by NIS since the service was started
	Connections Blocked by NIS/sec	The average number of connections blocked by NIS per second since the service was started
Forefront TMG Web Proxy:		
	Signatures blocked by NIS in last day	The total number of Web requests blocked by NIS in last day.
	Signatures detected by NIS in last day	The total number of Web requests detected by NIS in last day.
	Protocol anomalies detected by NIS in last day	The total number of protocol anomalies detected by NIS in last day.
	Protocol anomalies blocked by NIS in last day	The total number of protocol anomalies blocked by NIS in last day.

There are two additional NIS counters included in the "Forefront TMG Firewall Packet Engine" group ("Packets Blocked by NIS" and "Packets Blocked by NIS/sec") however they are not implemented in Forefront TMG 2010 and will always show a zero value.

Troubleshooting NIS

NIS Troubleshooting scenarios are divided into the following categories:

1. Signature set updates failure
2. Potentially incorrect detection
3. Potentially incorrect protocol anomaly detection
4. Potentially missing detection

Signature Set Updates Failure

To keep your systems protected from the latest threats, NIS must have connectivity to the appropriate update source (Microsoft Update or WSUS) and updated with latest signature sets. NIS will trigger an alert on any failure to update the latest signature set and display a warning on the Forefront TMG management console Alerts tab. When the signatures are up to date, the Update Center appears as follows::

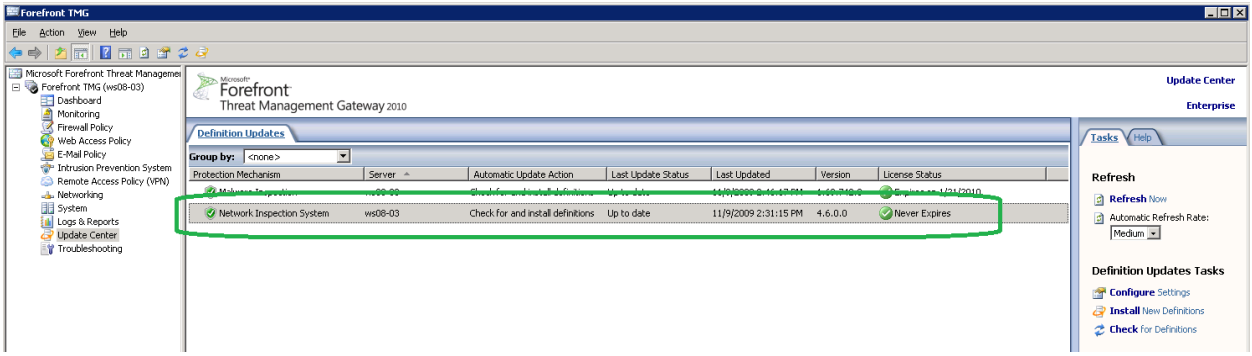


Figure 36: Forefront TMG Update Center

NIS will alert if it hasn't received updates for more than certain number of days. This number is configurable through the **NIS Tasks**. Select **Configure Properties** and then select the **Definition Updates** tab. This threshold is 45 days by default:

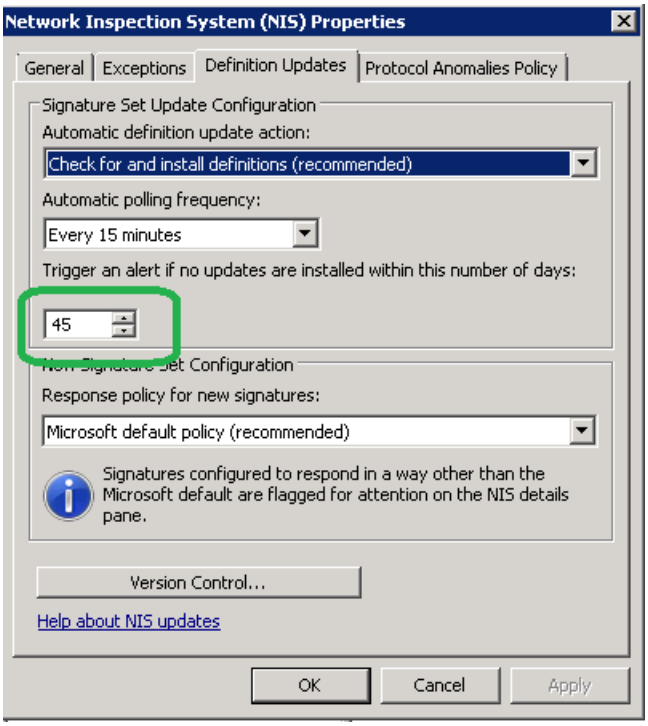


Figure 37: Threshold for triggering a "NIS signatures out of date" alert

The following table lists the possible NIS alerts for signature set updates along with the corresponding troubleshooting steps. The alerts are listed in the Forefront TMG management console Alerts tab. Select the **Monitoring** node in the left pane to see that tab.

Table 3: Troubleshooting signature updates

Name	Severity	Description	Troubleshooting Steps

#1	Update Failed	Error	An error occurred during an attempt to check for, download, or install definition updates on the server <server-name>	1. Check Forefront TMG connectivity to Microsoft Update 2. Verify WinHTTP proxy settings 3. Use the error code for further investigation
#2	NIS Signature Set Loading Failed	Error	NIS failed to load the signature set file on the server <server-name> because the current signature set file is missing or is corrupted.	Take the following steps: 1. Select the **Update Center** node in the left pane 2. Select the NIS entry in the **Definition Updates** pane 3. Select **Override Current Definitions**
#3	NIS Selected Signature Set Loading Failure	Error	The server <server-name> is configured to use the selected signature set <name> instead of the latest signature set retrieved by Forefront TMG but NIS will use the latest signature set because the selected signature set could not be loaded on the specified server.	To stop using the selected signature and start using the latest released signature, follow these steps: 1. Select the **Intrusion Prevention System** node in the left pane 2. Select **Configure Properties** from the **NIS Tasks** menu. 3. Select the **Definition Updates** tab 4. Click **Version Control…** 5. Uncheck **Select the NIS signature set you want to activate** option
#4	Update Center - Updates Not Installed	Warning	One or more protection mechanisms did not install updates during the last <number of days> days. Protection mechanisms that did not install updates: **Network Inspection System**. When a protection mechanism is configured to check for updates and not to install them automatically, available updates must be installed manually from the **Update Center**	To enable automatic updates: 1. Select the **Intrusion Prevention System** node in the left pane 2. Select **Configure Properties** from the **NIS Tasks** menu. 3. Select the **Definition Updates** tab 4. Set **Automatic definition update action** to **check for and install definitions (recommended)** 5. Set **Response policy for new signatures** to **Microsoft default policy (recommended)** To manually install update, 1. Select the **Update Center** node in the left pane

			node.	2. Select the NIS entry in the **Definition Updates** pane 3. Select **Check for and Install New Definitions** option from its right-click menu
#5	Update Center Required Service Not Started	Error	The Update Center cannot obtain updates on the server <server-name> because the Forefront TMG Job Scheduler service is not started.	1. Select the **Monitoring** node in the left pane 2. Select the **Services** pane 3. Right click **Microsoft Forefront TMG Job Scheduler** 4. Select **Start** (see screen shot below)

The following events about NIS updates are informational and are not indicative of any failure:

Table 4: Non-failure signature events

	Name	Severity	Description	Action
#1	NIS succeeded to load the signature set	Info	NIS succeeded to load the signature set	No action needed
#2	Definition Updates Installed	Info	One or more new definition updates for the Network inspection System were installed successfully on the server <server-name>. The new definitions are effective for new connections only.	No action needed
#3	Definition Updates Available	Warning	New definition updates for the Network inspection System on the server <server-name> are available, but they were not installed because Forefront TMG is configured to check for updates and not to install them automatically. The following updates are available for installation: <NIS, AM	You should turn on automatic updates: 1. Select the **Intrusion Prevention System** node in the left pane 2. Select **Configure Properties** from the **NIS Tasks** menu. 3. Select the **Definition Updates** tab 4. Set **Automatic definition update action** to **check for and install definitions (recommended)**

		...>	5. Set **Response policy for new signatures** to **Microsoft default policy (recommended)**

Potentially Incorrect Detections

In rare cases, NIS may incorrectly detect legitimate traffic as a potential threat and block it if configured to do so. The NIS team uses telemetry to constantly enhance the quality of protocol decoders. In particular, the MMPC uses telemetry to maintain high-quality signatures in order to minimize the impact of incorrect detections and quickly respond to such events. If an incorrect detection is found, the updates follow a roll-forward model. A revised signature is then created, tested, and published to supersede the previous one. This way, customers benefit from the protection against the other emerging threats that are addressed by the newer signature set. For information about the MMPC response please see the Understanding the Research and Response for NIS section.

If you suspect that a specific signature is causing incorrect detections, you should set the specific signature action to Detect only and report the issue to Forefront TMG Customer Support[2]. Some information, such as a network capture file, may be requested as part of an investigation. In the case that you had joined Microsoft Telemetry Service in Advanced Participation level, these reports will be helpful for the Microsoft Malware Protection Center team to analyze the incident and take action as necessary. Please see the Telemetry Service section for more information.

Potentially Incorrect Protocol Anomaly Detection

As discussed in the Configuring Protocol Anomalies Policy section above, this feature can help identify malicious traffic on your network. However there is some risk that protocol anomalies will trigger incorrect detections, especially in cases where applications were not implemented according to formal protocols specifications. When protocol anomaly detection occurs, both a log entry and alert are added.

In the example below, anomaly detection was triggered because the GET request specified invalid HTTP version of “1.2”. The log entry for this event is the same as other signature detection actions.

The Alerts tab shows the alert which was fired following this detection:

[2] For Customer Support options please refer to http://support.microsoft.com/contactus/?ws=support

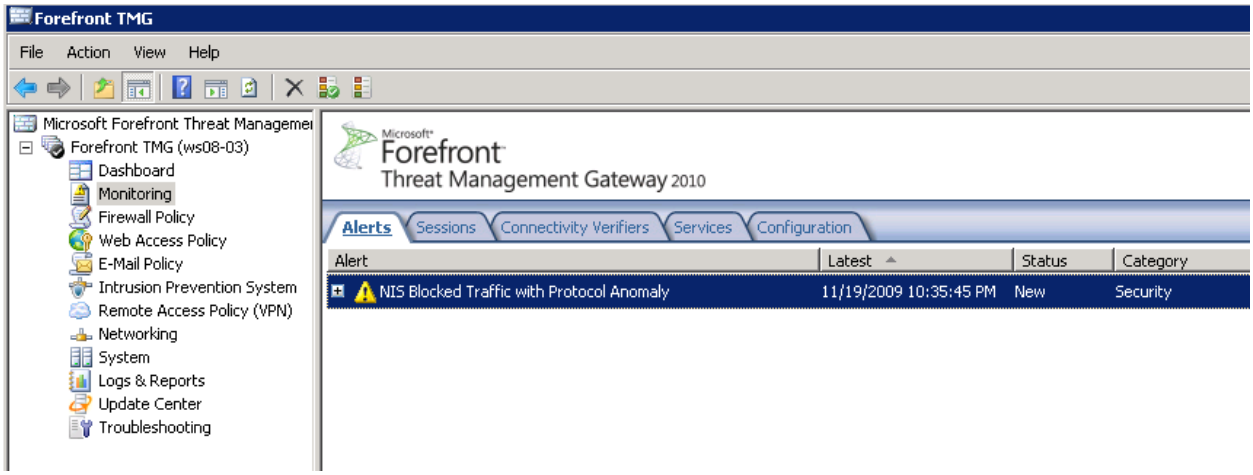


Figure 38: NIS alert for a policy anomaly detection

Here is the specific alert text:

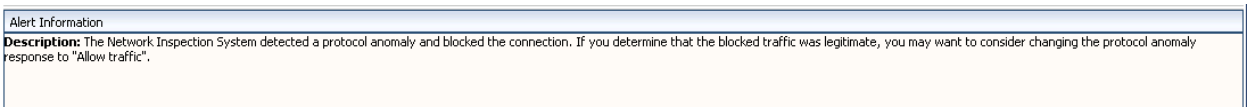


Figure 39: Protocol Anomaly Alert Text

When Telemetry Reporting is enabled, NIS will report the incident to MMPC to help identify and eliminate potential similar detections in the future.

When Forefront TMG alerts indicate that the session was blocked due to protocol anomaly, you may consider changing the Protocol Anomalies Policy to allow traffic instead of blocking it. To do that, follow these steps:

1. Select the **Intrusion Prevention System** node in the left pane
2. Select **Configure Properties** from the **NIS Tasks** menu.
3. Select the **Protocol Anomalies Policy** tab
4. Select the **Allow, to avoid blocking legitimate traffic** option.

Potentially Missing Detection

The following section discusses potential reasons for lack of detection for an apparent exploit, sometimes referred to as a false negative.

File Based Exploits

NIS helps protect against network based attacks and against some Web based attacks, however it doesn't provide protection against exploit files (file based attacks). Protection for exploit files is provided by Forefront TMG Malware Inspection. If you are investigating a case where an exploit file managed to penetrate through Forefront TMG, make sure Forefront TMG Malware Inspection is enabled and updated. Refer to the Forefront TMG help file for further information.

Signature Policy Configuration

Exploits may not be detected due to the configured policy. In the case where an exploit is not blocked by a corresponding NIS signature, you should check that signature policy settings. Make sure that the signature is not disabled or set to Detect only. If it is, enable or set it to Block.

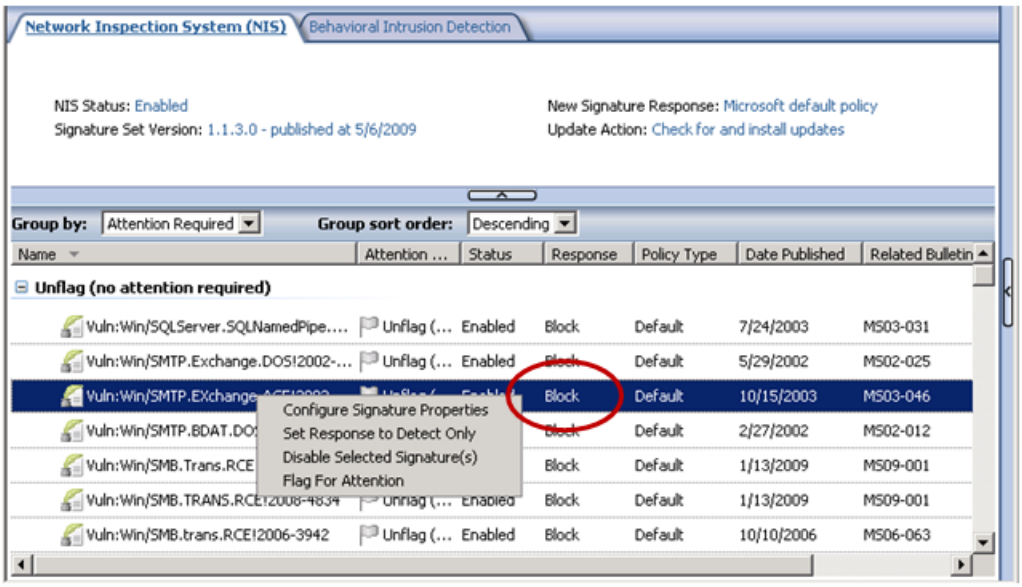


Figure 40: NIS signature response action

Network Object Exception

Another possible reason for an apparently missing detection is a configured NIS exception. Exceptions can exclude certain networks, computers, IP address ranges etc. from interception. See the Configuring Exceptions section for details.

Signature Set Version is not Up-to-date

An exploit may not be detected if NIS doesn't use the latest signature set. You should verify that NIS is up-to-date with the latest signature set. See the Signature Set Updates Failure section for details.

User Defined Protocols

Only the protocols that are listed in the NIS UI are inspected by NIS. In the case that a user defined protocol (using non-standard ports) has been added, it must be associated with a standard protocol. Once a non-standard protocol is added, follow these steps to associate it with a standard protocol:

1. Select the **Firewall Policy** node in the left pane
2. Expand the **User-Defined** entry on the **Protocols** list in the **Toolbox** on the right
3. Right click the non-standard protocol and select **Properties**
4. Select the **Associate this protocol definition with this standard protocol** option
5. Choose the standard protocol from the drop down list

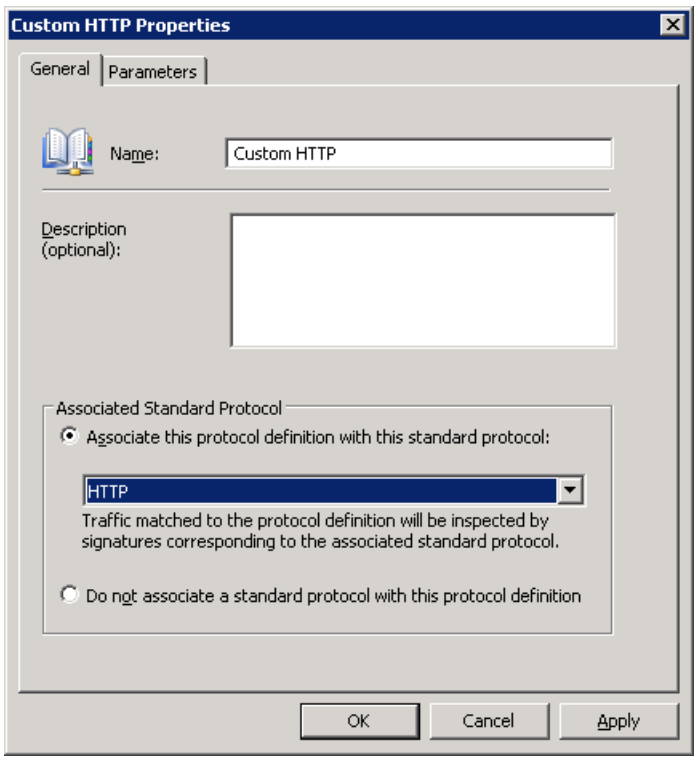


Figure 41: Associating a user defined protocol with a standard protocol

Note that the following conditions must be met for creating such an association:

- The secondary connections of the user-defined protocol must be a subset (or all) of the secondary connections of the predefined standard protocol.
- The same application filters must be selected for the standard protocol and for the user-defined protocol. For example, because the standard HTTP protocol is handled by the Web Proxy Filter, only if the user-defined "Custom HTTP" protocol is configured to use that filter, will it be possible to select the HTTP protocol from the list of protocols.

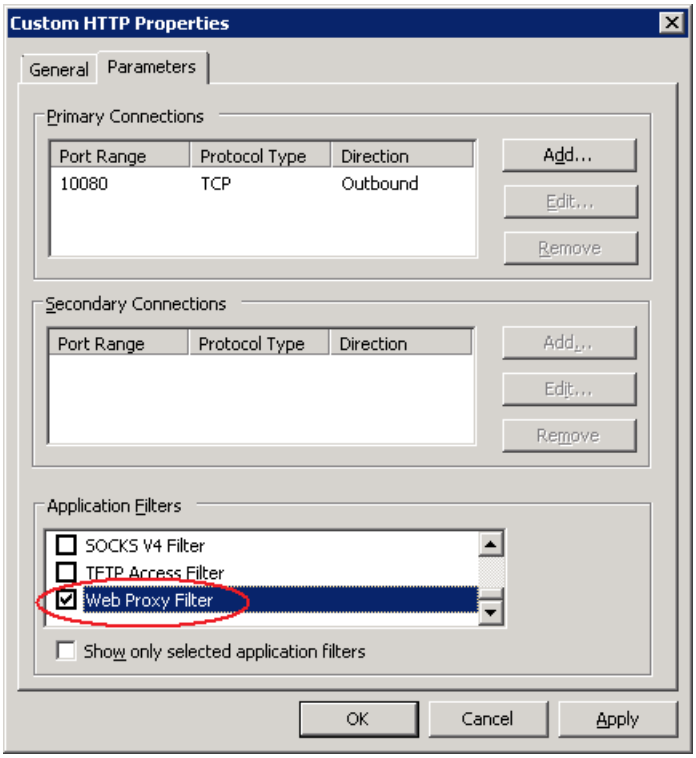


Figure 42: Selecting the application filter

Detection Related NIS Alerts

Here is the list of NIS alerts for detection issues. These alerts are informational and do not necessarily indicate any problem.

Table 5: NIS detection alerts

	Name	Severity	Description	Action
#1	NIS blocked traffic	Info	The Network Inspection System blocked traffic because it matched the vulnerability signature <Signature Name>. See the log for more details. Additional information about the signature can be found at <URL>. The currently installed Network Inspection System set version is <version>.	If there is reason to believe that the session block is inaccurate, consider setting the signature to Detect Only and report the issue to Forefront TMG Customer Service. See the Potentially Incorrect Detections section for more details.
#2	NIS detected traffic	Info	The Network Inspection System detected traffic that matches the vulnerability signature	You should use the default response policy: 5. Select the **Intrusion**

			<signature name>. The traffic was not blocked because the signature is configured for detection only mode. See the log for more details. Additional information about the signature can be found at <URL>. The currently installed Network Inspection System set version is <version>.	**Prevention System** node in the left pane 6. Select **Configure Properties** from the **NIS Tasks** menu. 7. Select the **Definition Updates** tab 8. Set **Response policy for new signatures** to **Microsoft default policy (recommended)** For a specific signature that is configured to use non-default response: 1. Select the **Intrusion Prevention System** node in the left pane 2. Double click on that signature 3. In **General** tab, configure the signature to use response policy **Microsoft default (recommended)**
#3	NIS blocked traffic because it detected a protocol anomaly	Info	The Network Inspection System blocked traffic because it detected a protocol anomaly. See the log for more details. The currently installed Network Inspection System set version is <version>.	If there is reason to believe that the session block is inaccurate, consider modifying the Protocol Anomalies Policy to allow traffic by following these steps: 1. Select the **Intrusion Prevention System** node in the left pane 2. Select **Configure Properties** from the **NIS Tasks** menu. 3. Select the **Protocol Anomalies Policy** tab 4. Select the **Allow, to avoid blocking legitimate traffic** option.

Tools and Tips

Viewing History of Configuration Changes

Forefront TMG provides the ability to view the list of configuration changes. You may find this feature helpful when testing your Forefront TMG configuration or when troubleshooting. To view history of changes:

1. Select the **Troubleshooting** node from the left pane
2. Click the **Change Tracking** tab

You will get a list of all the configuration changes that were applied to Forefront TMG. In order to limit the changes only to those that pertain to NIS, configure the filter at the top to look only for changes where the entry contains NIS as shown below, and then click **Apply Filter.**

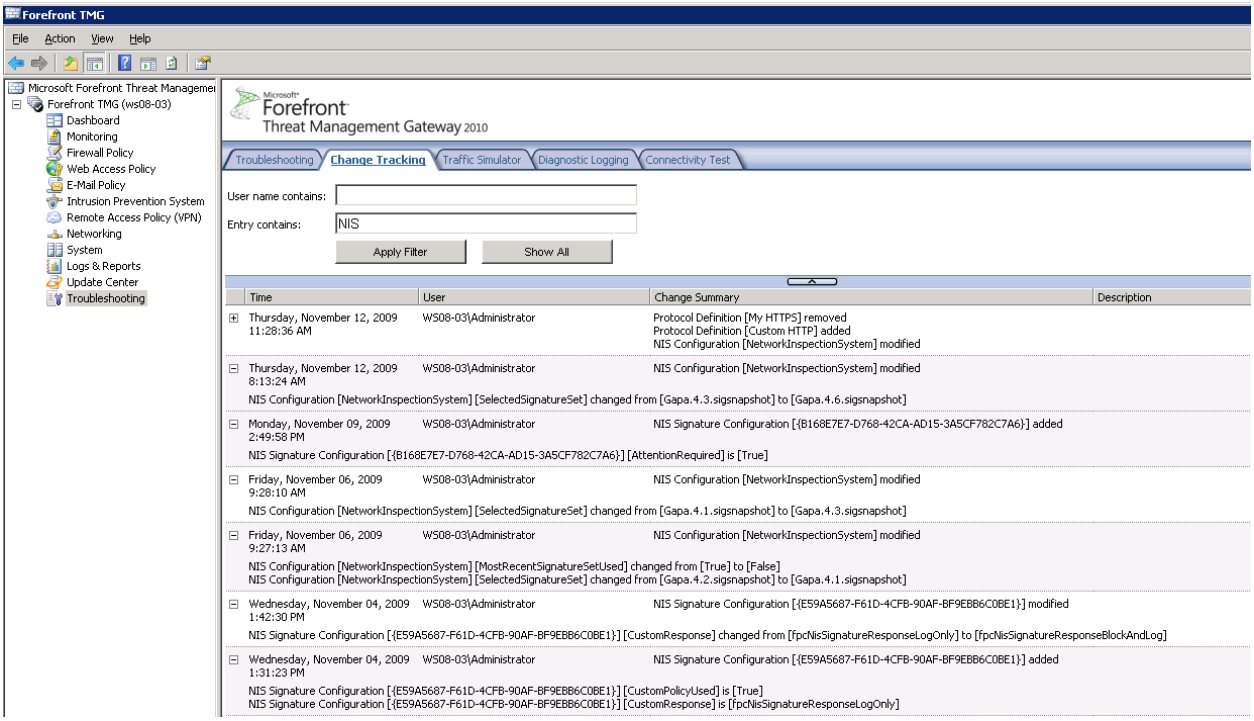


Figure 43: Viewing the list of configuration changes for NIS

Using Windows Event Viewer:

All NIS and Forefront TMG alerts can be configured to trigger events in the Windows Application event log. For example, here is an event that was triggered by detection of the HTTP test signature (see the Testing NIS Deployment section for details).

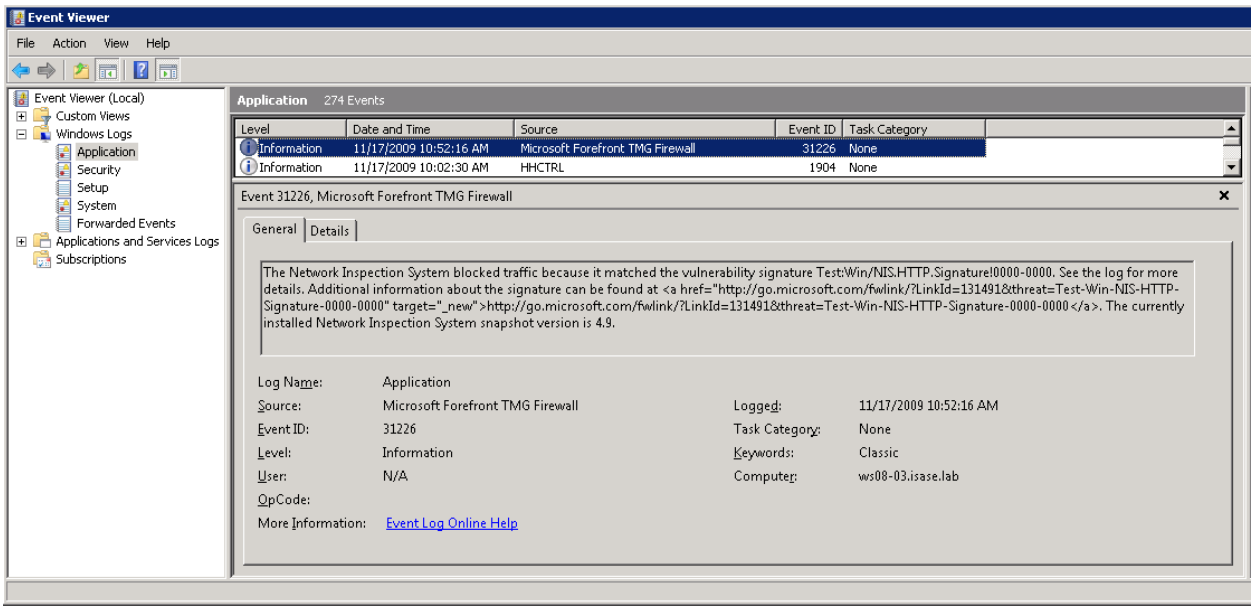


Figure 44: NIS blocking event

Using Forefront TMG Logs

Forefront TMG logs include special fields to support NIS:

- **Signature Name**: The NIS signature name correlates the log entry to the corresponding signature.
- **NIS Scan Result**: This field indicates whether a session was inspected by NIS and the result of this inspection. The possible values are:
  - **Inspected** –Inspected and allowed by Forefront TMG
  - **Detected** – Detected by NIS <Signature Name> but allowed due to policy set to "Detect Only"
  - **Blocked** - Detected by the NIS <Signature Name> and rejected.
- **NIS Application Protocol** – The particular protocol for which the signature was detected. The application protocol could be layered, such as in an RPC over HTTP session. In that case, the NIS Application Protocol will be RPC while the Firewall protocol will be HTTP.

Additional information that assists in analyzing Forefront TMG logs for NIS:

- Firewall logs indicate sessions inspected by NIS only when the connection is closed, either by a firewall action or by the client/server action.
- When a connection is blocked due to protocol anomaly detection, the NIS Application Protocol and Signature Name fields will be empty.

Understanding the Research and Response for NIS

NIS in Forefront TMG is backed by a world class Threat Research and Response team in the Microsoft Malware Protection center (MMPC). The MMPC is committed to providing customers with

comprehensive protection against exploitation of vulnerabilities in addition to viruses, spyware, and other new and existing malware. This organization is composed of a dedicated group of experienced researchers and Microsoft security technologists that are responsible for researching and responding to new threats, as well as providing the necessary security technology and infrastructure to protect customers.

The MMPC uses a research and response process through which it monitors submissions and reports from around the world, analyzes suspect reports and delivers updates providing the latest protection. This team also conducts research aimed at utilizing state-of-the-art static and dynamic analysis techniques to automate the process of identifying vulnerabilities in binaries and developing signatures without access to source or debug information.

The figure below shows a high-level view of the process followed by the MMPC.

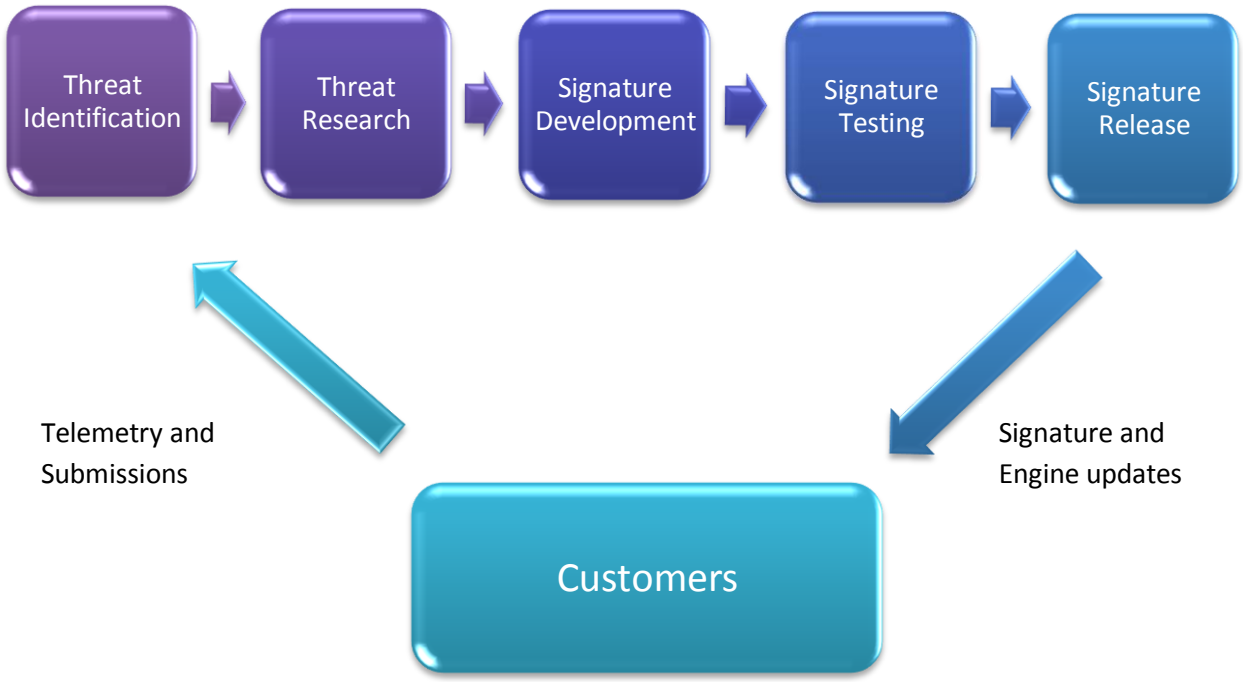


Figure 45: Overview of the threat research and response process

Threat Identification

The first stage of the analysis process is to gather reports on new vulnerabilities and attacks. This information can come from many channels, such as automated monitoring tools, product support or collaboration with industry partners. Additionally, a large amount of useful data is often submitted by customers, based on issues they're seeing on a day-to-day basis.

A critical aspect in defining the response to a new threat is determining its severity. This table shows the definitions for the rating systems used.

Table 6: Threat severity ratings

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user's data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Threat Research

In order to develop a signature against a vulnerability, it is important to understand how the vulnerability could be exploited. An environment is set up where the vulnerability can be consistently reproduced and root cause analysis is performed. Based on this determination, conditions are extracted that will help detect exploits against the vulnerability on the network. The MMPC combines existing data with automated and manual analysis techniques to quickly respond to current and emerging threats.

Signature Development

After the vulnerability is analyzed, the final output is a signature used by the NIS engine to detect and block network based attacks. The type of the signature developed is determined according to the results of the research.

Signature Testing

After the signature is created, it undergoes various tests to help ensure that it functions as expected. The signature is tested against collections of network captures to help ensure it detects threats correctly

Signature Release

Once the signatures have been certified through testing, they are digitally signed and packaged for distribution to Microsoft Update servers. The digital signature guarantees the authenticity and integrity of the file, and the distribution packaging creates various full and partial updates for the client. Depending on how frequently a client updates, it may only need to install a small change to the definitions rather than a complete update.

In addition, an encyclopedia entry is released to the Microsoft Malware Protection Center portal that provides customers with additional details about the vulnerability itself.

Figure 46: Detailed threat research and response process

The customer is a critical part of the feedback loop for the research and response team. Customers can choose to send telemetry to the MMPC for analysis. The active involvement of customers in the research and response process provides insight into current trends, enabling the MMPC to respond quickly with updates to help protect customers. For more details about the telemetry, please see the Telemetry Service section.

Rapid Response

The team performs rigorous analysis on collected data through a combination of automation, security expertise, and testing processes to identify the latest threats. This approach involves significant investment in automation to efficiently use researcher resources and deliver rapid response. An example of this automation is Paladin[3] – a set of tools that help support rapid and scalable vulnerability analysis and signature development.

The motivation behind this work is to automate the otherwise laborious process of analyzing exploits, identifying malicious input bytes, determining how shell code is executed and thus narrowing the search space for further manual analysis. The ability to respond quickly to an emerging threat is critical, so the research team must be able to address a variety of exploits and vulnerabilities efficiently.

This global team delivers guidance to customers through an integrated communications approach with Customer Support Services (CSS) to respond quickly to customer issues and provide customer guidance.

[3] For details about Paladin, see the following blog post: http://blogs.technet.com/mmpc/archive/2009/04/15/an-introduction-to-mmpc-paladin-automated-vulnerability-analysis.aspx.

The MMPC Web portal (http://www.microsoft.com/security/portal/) delivers up-to-date information about current threats, news and MMPC research. Customers can get key insights on the top threats in the online encyclopedia.

The figure below shows a sample encyclopedia entry:

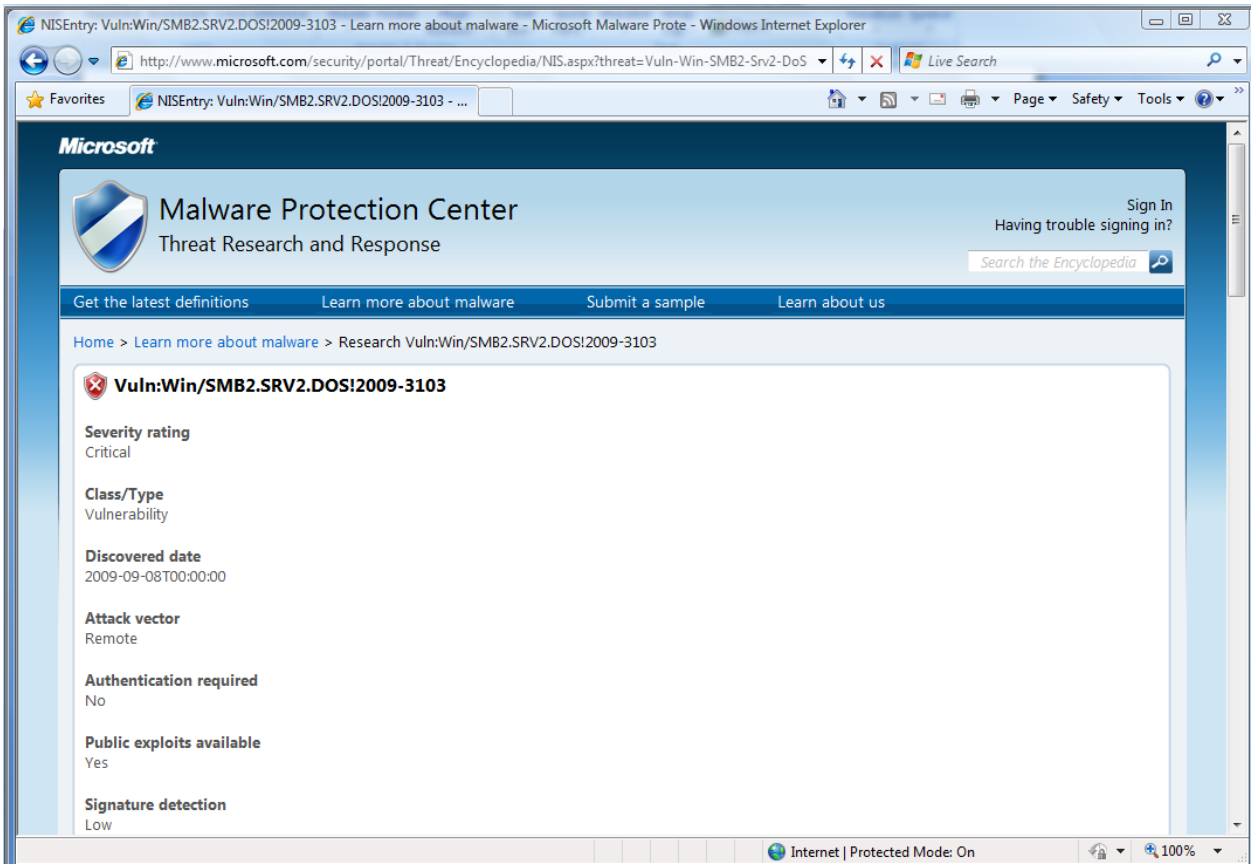


Figure 47: Sample encyclopedia entry

Concluding Thoughts

The threat landscape is changing quickly. Threats continue to evolve, becoming more advanced as the criminals are motivated by financial gain. Microsoft is committed to help protect customers from current and emerging threats, while fostering security industry collaboration for the benefit of the computing ecosystem.

Through an experienced team, combined with advanced telemetry, automation, and integrated processes, the MMPC delivers global research and response in a reliable, accurate, efficient and consistent manner to address the needs of its customers.