Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront TMG – Using the BranchCache feature in Forefront TMG SP1

Abstract

In this article I will show you one of the new features in Forefront TMG Service Pack 1 called BranchCache in Hosted Mode.

Let's begin

Forefront TMG SP1 supports configuring the Server as a BranchCache Server in Hosted Mode. BranchCache is not used exclusively with Forefront TMG. BranchCache is a feature first introduced in Windows Server 2008 R2 and Windows 7 which use techniques to reduce the amount of data transferred from the Headquarter to the Branch Office through a WAN link. BranchCache provides two operation modes:

- Distributed Cache
- Hosted Cache

Distributed Cache

The Distributed Cache feature is great for small Branch Office without a dedicated Server. The BranchCache will be distributed between several Windows 7 clients, where every Windows 7 client hosts part of the BranchCache content.

Hosted Cache

In the Hosted Cache Mode there is a dedicated Server which hosts the cached content of the BranchCache. Every Windows 7 client in the BranchOffice can participate from the central cache in Hosted Cache mode. The Hosted Cache mode operates by deploying a computer that is running Windows Server 2008 R2 as a host in the Branch Office. If the content is not available in the Hosted Cache, it is retrieved from the content server by using the WAN. The Hosted Cache Mode server stores the content locally so that subsequent client computers can benefit from the Hosted cache again.
To deploy BranchCache in Hosted Cache mode, you must install and configure content servers in your main office, and install and configure a Hosted Cache server and client computers in your branch office.

Note:

Forefront TMG SP1 can only be configured to operate in Hosted Cache Mode.

Activating BranchCache on Forefront TMG SP1

BranchCache in Hosted Cache mode can be activated in the Forefront TMG Management console. Navigate to the Firewall policy node and on the Task pane click *Configure BranchCache* and enable BranchCache in Hosted Cache mode.

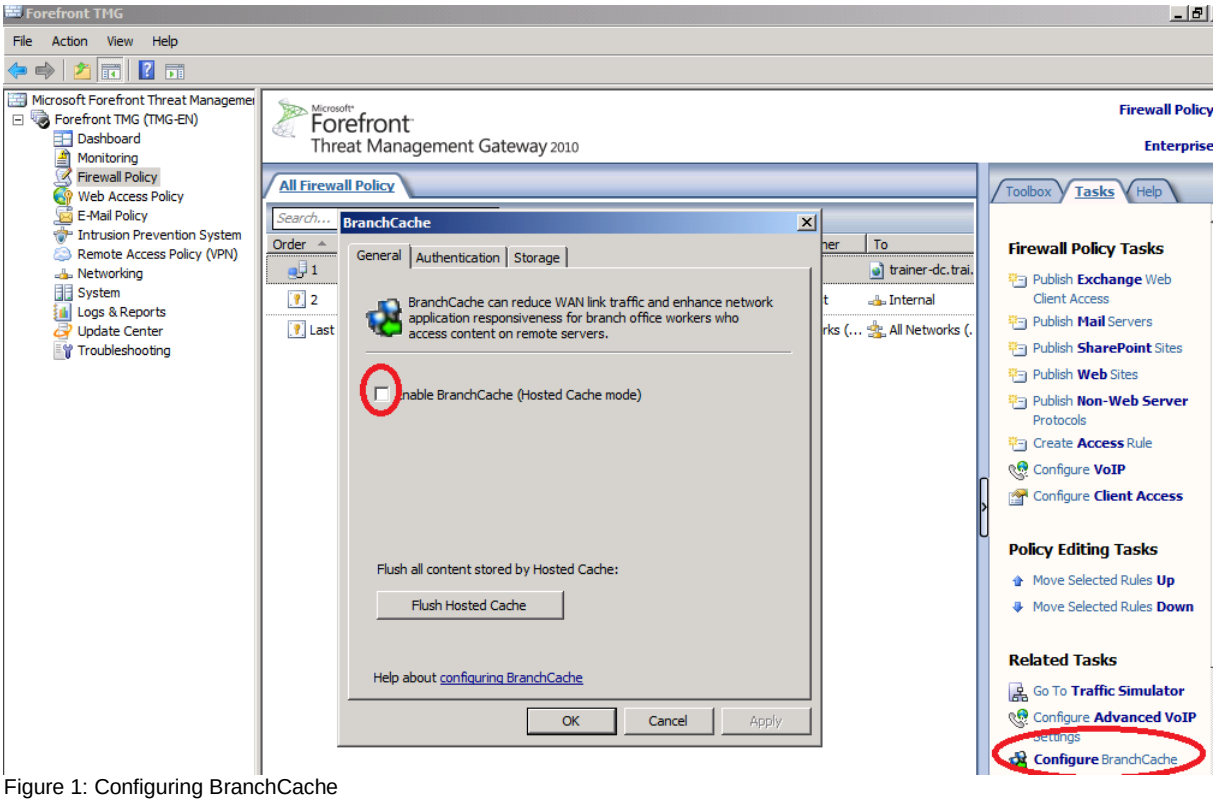


Figure 1: Configuring BranchCache

Hosted Cache authentication

The Hosted Cache is trusted by client computers to cache and distribute data that may be under access control to prevent executing and reading the data. To enhance the security, Windows 7 client computers use Transport Layer Security (TLS) when communicating with the Hosted Cache server. To support a TLS connection, Forefront TMG must have a certificate that is trusted by clients and the Extended Key Usage (EKU) must be server authentication. So the next step is to issue a Computer certificate from an internal certification authority (CA) which is trusted by all domain members. For the certificate in this article we are using the MMC on the Forefront TMG Server to request a certificate with the Computer certificate template. The Common Name (CN) of the certificate is the FQDN of the Forefront TMG Server.

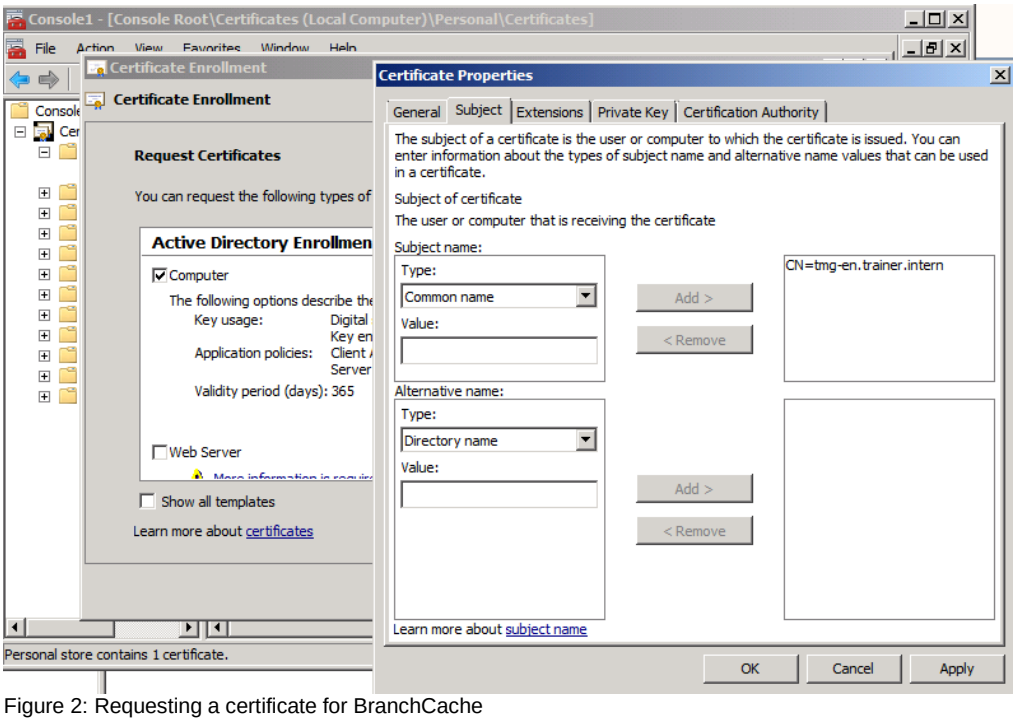


Figure 2: Requesting a certificate for BranchCache

After the certificate is issued and stored in the certificate store of the local computer, we can use the certificate to encrypt the data transfer from the Hosted Cache. Selected the certificate and if you only want to allow clients from the same Windows domain to access the Hosted Cache, activate the checkbox, as shown in the following picture.

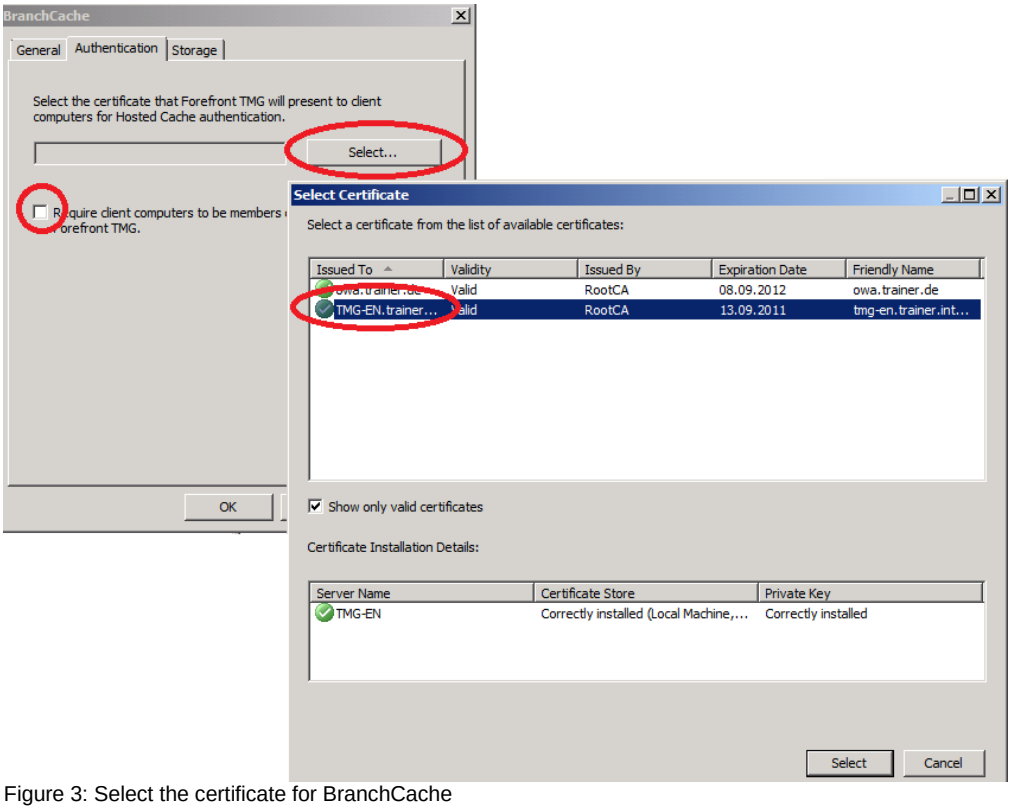


Figure 3: Select the certificate for BranchCache

BranchCache in Hosted Mode store the content of the Hosted Cache on the disk of Forefront TMG. I recommend using a dedicated volume or disk for Hosted Cache content and not the default folder. If you use a dedicated volume or disk you can also increase the percentage storage used for the Hosted Cache. The default value is 5 percent and I increased the percentage to 90 percent to keep 10 percent as a reserve.

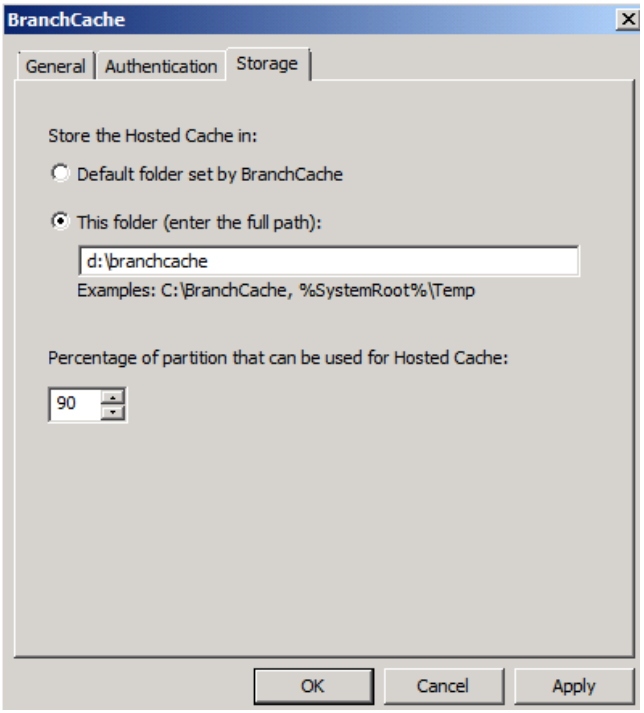


Figure 4: Select the location for BranchCache content and the Percentage of disk space used for Hosted Cache.

NIS Inspection and BranchCache

The next step is optional but very important in my opinion if you use the Network Inspection System (NIS) feature in Forefront TMG. TMG is a vulnerability-based Intrusion Prevention System (IPS). An IPS should protect your internal network from known and unknown vulnerabilities if TMG is being used directly on the edge of the internal network on the Internet. All network traffic must flow through TMG, so TMG is the first line of defense to protect against different vulnerabilities. TMG NIS IPS features block un/known attacks at the network level to fight against vulnerabilities. TMG uses a signature based IPS. A signature based IPS protects your hosts against exploitation of vulnerabilities which are found. A signature based IPS is used to close the time window between an announcement of vulnerability and the patch deployment of all possible vulnerable hosts.
When NIS is enabled all traffic gets inspected, including traffic destined explicitly to the host or originating from the host. As a result, it may be possible that users may experience an increased latency when retrieving objects from the Hosted Cache server.
To improve the performance it is possible to disable NIS for traffic from or to the Host to disable NIS for traffic to the host or originating from the host.

Attention:

Disabling NIS in Forefront TMG decrease the protection mechanism of Forefront

TMG. You will find more information about possible security impacts in the guide for implementing BranchCache with Forefront TMG. You will find a link to this guide at the end of this article.
With the following registry key it is possible to disable the NIS traffic inspection of the Localhost:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RAT\Stingray\Debug\IPS\IPS_LOCALHOST_INSPECTION_MODE – Set the value to 0.

After that you must reapply the Forefront TMG policy.

Next we have to change the BranchCache protocols default port numbers (from port 80 and 443) to custom port numbers. By default NIS inspects only HTTP and HTTPS on Localhost traffic. To retain inspection for non-related Branchcache traffic without impacting BranchCache performance it is required that the BranchCache default ports are changed to another available port.

Firewall Rules for BranchCache

By default, Forefront TMG blocks most traffic that is destined explicitly to the Forefront TMG Server or originating from the TMG Server, so we have to modify the Forefront TMG Firewall rules to allow BranchCache traffic because BranchCache is operating in Hosted Mode on the Forefront TMG Server.

A BranchCache client initiates a connection to the Forefront TMG Server with the Hosted Cache Protocol (PCHC – Port 443). The Hosted cache Server will initiate a new connection using the Retrieval protocol (PCCRR – Port 80) to retrieve the data from the client. After that the data is now cached on the Hosted Cache Server. Another BranchCache client that needs to retrieve data from the Hosted Cache will initiate the Retrieval protocol (PCCRR) and retrieve content from the Hosted Cache. To allow this communication you must define two Forefront TMG policy rules:

- Allow Hosted Cache Inbound Connections
- Allow Hosted Cache Outbound Connections

Allow Hosted Cache Inbound Connections

This Firewall rule allows BranchCache clients to advertise new content to the Hosted Cache Server and retrieve data from the Hosted Cache Server.

Allow Hosted Cache Outbound Connections

This Firewall rule allows the Hosted Cache Server to retrieve advertised content from the BranchCache client.

The actual ports that are used by the BranchCache clients are stored in the Registry of the client. The Registry keys are located here:

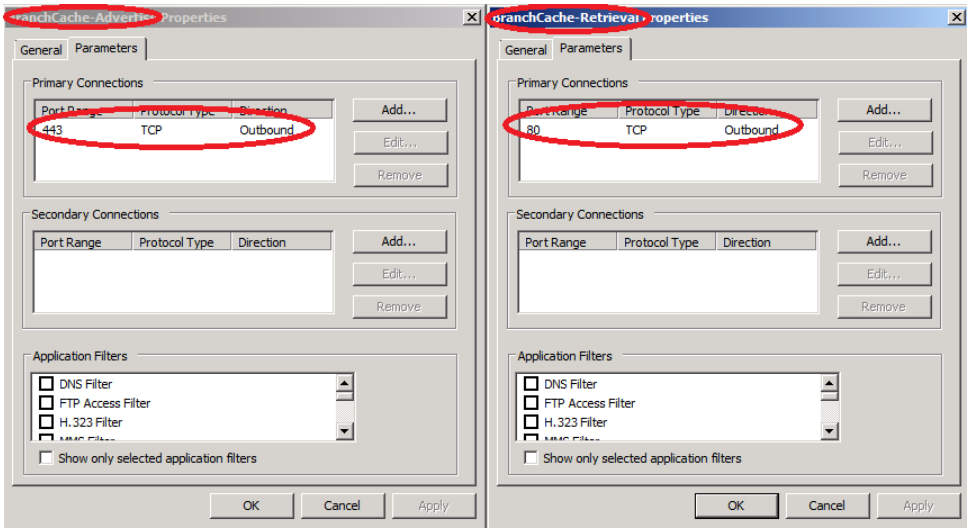
For the Retrieval port (Default is Port 80)

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\PeerDist\DownloadManager\Peers\Connection

For the Hosted Cache port (Default is 443)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\PeerDist\HostedCache\Connection

Next we have to create the Firewall rules on Forefront TMG. You will see the Firewall protocol defintions in the following picture.



After the new Protocol definitions have been created we must create two new Firewall rules which allows traffic for these protocol definitions from the internal network to the Localhost Network and vice versa.

Figure 5: Firewall Protocol rules for BranchCache

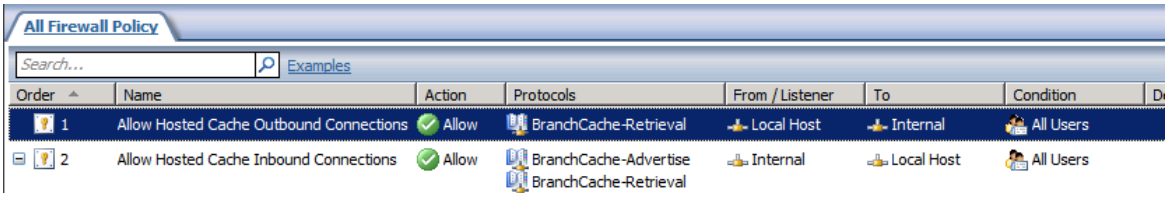


Figure 6: firewall rules for BranchCache

Click *Apply* to save the configuration changes to the Forefront TMG storage.

Monitoring BranchCache

There are many ways to monitor the BranchCache efficiency. One way is to use a new monitoring option in the Forefront TMG dashboard as shown in the following picture. Another way is to use the built-in Performance Monitor counters for BranchCache of Windows Server 2008 R2.

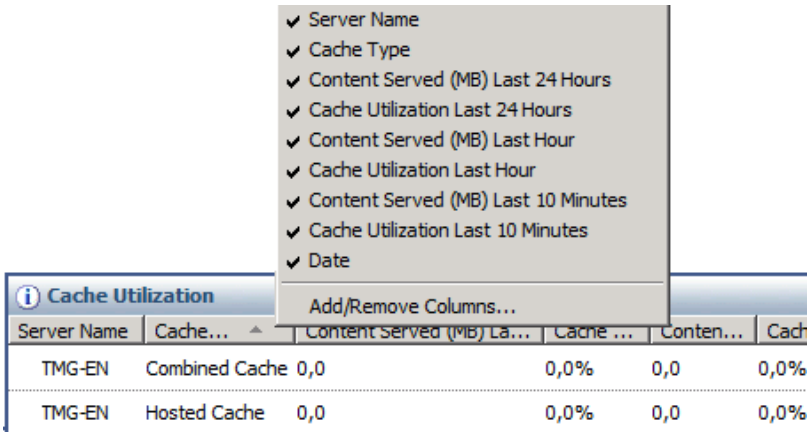


Figure 7: Monitoring BranchCache

BranchCache Performance Counter

Windows Server 2008 R2 comes with a lot of built-in Performance Counters to monitor the efficiency of the BranchCache feature on Forefront TMG. You will need to monitor these Performance Counters from time to time to make changes when the efficiency of the BranchCache doesn't fulfill your needs. To monitor the BranchCache performance start the Windows Server 2008 R2 Performance Monitor and select the BranchCache counters and add the Performance Counters to be monitored.

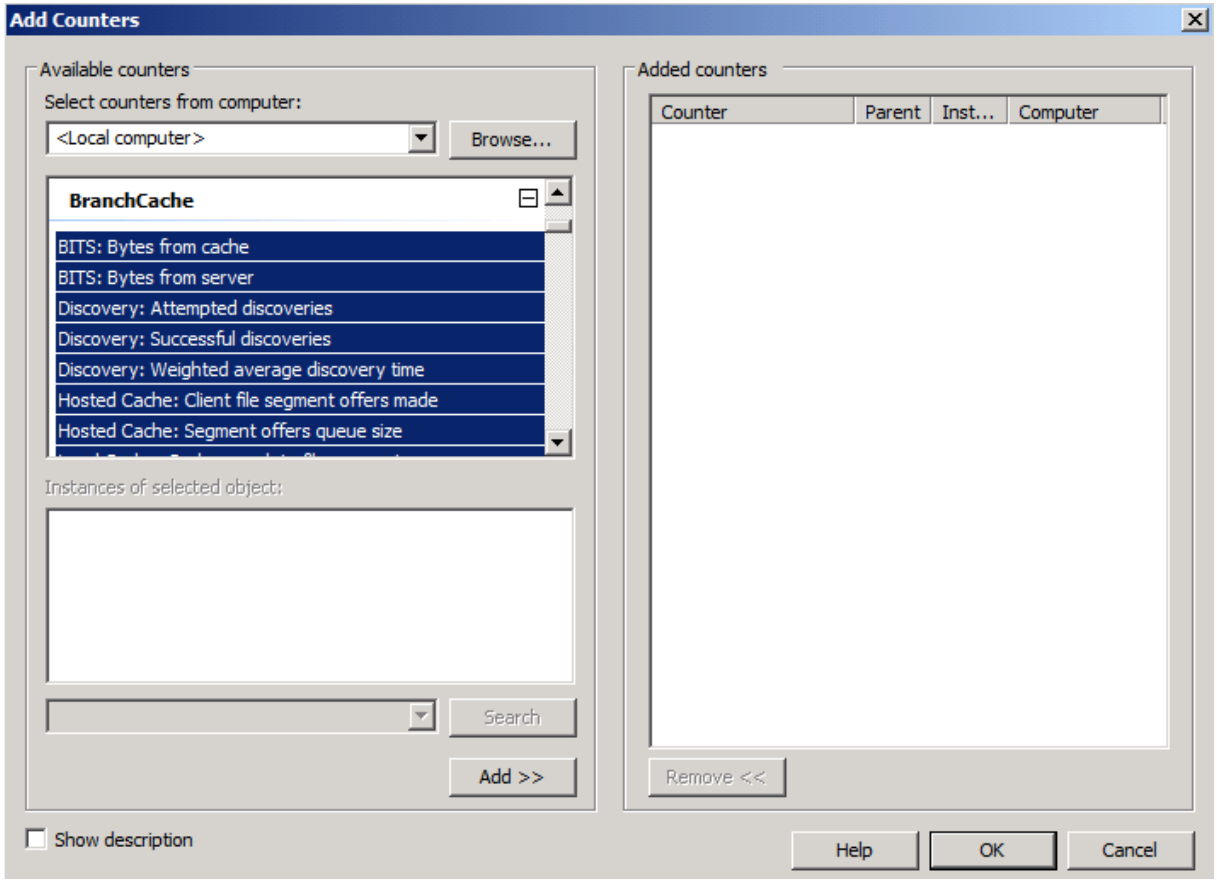


Figure 8: Performance Counters for BranchCache

Conclusion

In this article I tried to show you how to configure Microsoft Forefront TMG SP1 as a Hosted Server for BranchCache. With the help of the BranchCache feature you can use Forefront TMG without an additional Server or Server feature to fulfill the requests for Branch Office to get the most updated content directly from the Forefront TMG Server without overloading the WAN link. With the help of Forefront TMG it is easy to implement an integrated BranchCache solution which is also easy to monitor with the built-in Forefront TMG dashboard or the integrated Performance Monitor counters from Windows Server 2008 R2.

Related links

Planning for BranchCache (SP1)
http://technet.microsoft.com/en-us/library/ff685650.aspx
Performance Counters
http://technet.microsoft.com/en-us/library/dd637826(WS.10).aspx
Explaining and configuring NIS (Network Inspection Service)
http://www.isaserver.org/tutorials/Explaining-configuring-NIS-Network-Inspection-Service.html