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

How to use the ISA Server 2006 Network Templates

Abstract

In this article, I will show you how to use the ISA Server 2006 network templates to build your own ISA Server 2006 network infrastructure. I will also show you the technique behind network templates and how to customize these templates.

Let’s begin

Microsoft ISA Server 2006 is a Multilayer Firewall to control access between networks. ISA Server 2006 uses the following objects to establish connections between networks and to control the network traffic between these networks:

- Networks
- Network rules
- Firewall rules

Networks

ISA Server uses a multi network model which allows ISA Server Administrators to illustrate every physical network to which ISA Server is connected.
You first have to create networks as a basic element in ISA Server 2006.

Network rules

After the ISA Administrator defined all necessary networks, these networks must be brought in relationship between networks where network traffic should flow through. With ISA Server 2006 it is possible to establish two different types of network rules:

- Route
- NAT

Route

A network rule from type Route establish a bidirectional network connection between two networks which routes the original IP addresses between these networks.

NAT

A network rule from type NAT (Network Address Translation) establish a unidirectional network connection between two networks which substitutes IP addresses from the network segment with the IP address of the corresponding ISA Server network adapter.

Firewall rules

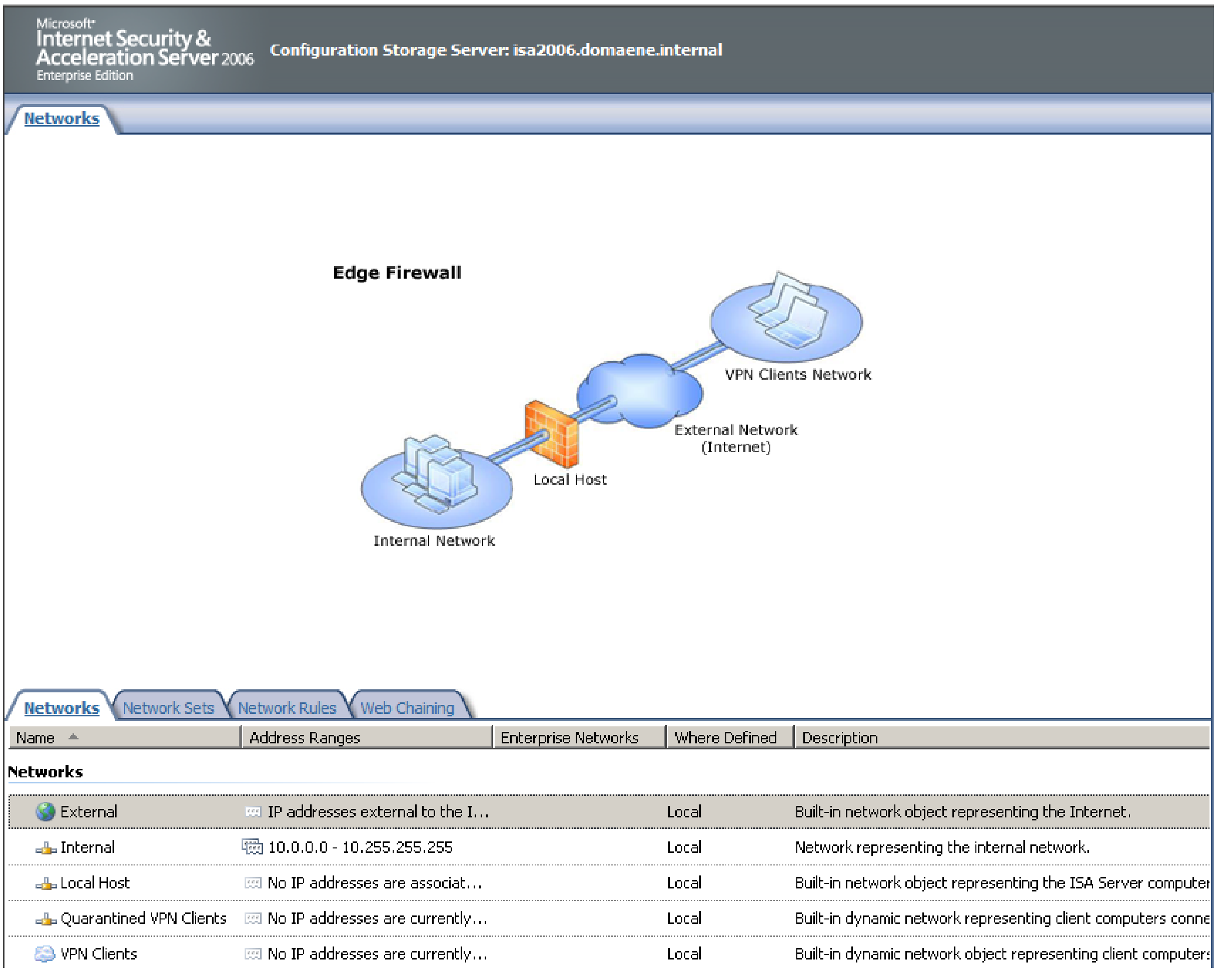
After all networks and necessary network rules are defined, you must control the network traffic between these networks with Firewall rules.

Overview about Networks in ISA

To get an overview about the ISA Server network configuration, start the ISA Server MMC, navigate to the *Configuration – Networks* node. You can see here four different tabs:

- Networks
- Network Sets
- Network Rules
- Web Chaining

The tab *Networks* lists all networks defined on ISA Server, *Network Sets* groups networks to a network group, *Network rules* define a Route or NAT relationship between networks and *Web Chaining* create a Web routing for web requests.



Configuration Storage Server: isa2006.domaene.internal

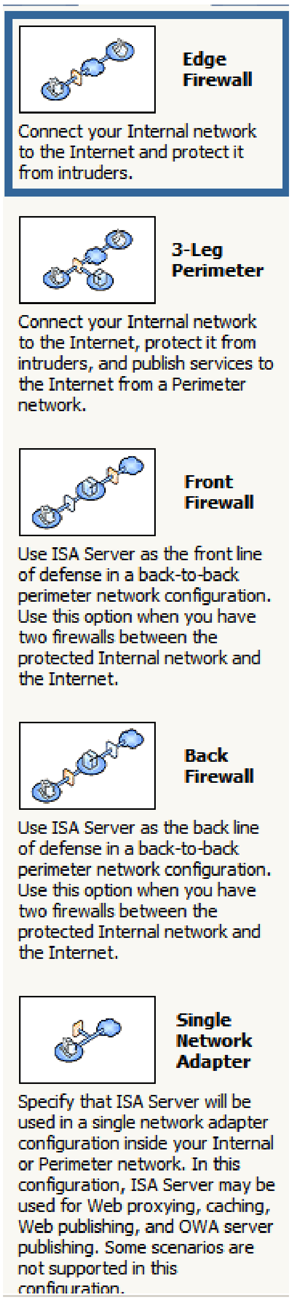
Name	Address Ranges	Enterprise Networks	Where Defined	Description
Networks				
External	IP addresses external to the I...		Local	Built-in network object representing the Internet.
Internal	10.0.0.0 - 10.255.255.255		Local	Network representing the internal network.
Local Host	No IP addresses are associat...		Local	Built-in network object representing the ISA Server computer
Quarantined VPN Clients	No IP addresses are currently...		Local	Built-in dynamic network representing client computers conne
VPN Clients	No IP addresses are currently...		Local	Built-in dynamic network object representing client computers

Figure 1: ISA Server 2006 networks

Right on the Task Pane you will find the templates tab. The templates tab lists all available network templates which ISA Server Administrators can use to build their own networks.

There are five templates available:

- Edge Firewall
- 3-Leg Perimeter
- Front Firewall
- Back Firewall
- Single Network Adapter



Edge Firewall

Connect your Internal network to the Internet and protect it from intruders.

3-Leg Perimeter

Connect your Internal network to the Internet, protect it from intruders, and publish services to the Internet from a Perimeter network.

Front Firewall

Use ISA Server as the front line of defense in a back-to-back perimeter network configuration. Use this option when you have two firewalls between the protected Internal network and the Internet.

Back Firewall

Use ISA Server as the back line of defense in a back-to-back perimeter network configuration. Use this option when you have two firewalls between the protected Internal network and the Internet.

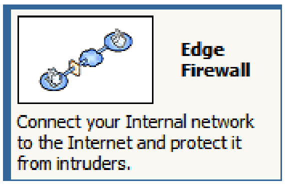
Single Network Adapter

Specify that ISA Server will be used in a single network adapter configuration inside your Internal or Perimeter network. In this configuration, ISA Server may be used for Web proxying, caching, Web publishing, and OWA server publishing. Some scenarios are not supported in this configuration.

Figure 2: ISA Server 2006 network templates

Edge Firewall

The Edge Firewall template is the classic network template and connects the internal network to the Internet, protected by ISA Server.



Edge Firewall

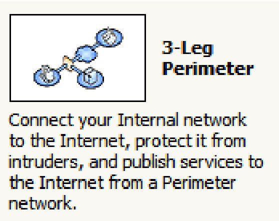
Connect your Internal network to the Internet and protect it from intruders.

Figure 3: ISA Server 2006 – Edge Firewall network template

A typical Edge Firewall template requires two network Adapters on the ISA Server. For more information about the Edge Firewall template, read the article from Tom Shinder called: Using ISA Server 2004 Network Templates to Automatically Create Access Policy: The Edge Firewall Template

3-Leg Perimeter

The 3-Leg Perimeter Firewall is an ISA Server with three or more network Adapters. One network adapter connects the internal network, one network adapter connects to the external network, and one network adapter connects to the DMZ (DeMilitarized Zone), also called Perimeter Network. The Perimeter network contains services, which should be accessible from the Internet but also been protected by ISA Server. Typical services in a DMZ are Web Servers, DNS Servers and something more. A 3-Leg Perimeter Firewall is also often called the “Poor Man’s Firewall”, because it is not a “true” DMZ. A true DMZ is the zone between to (possible) different Firewalls.



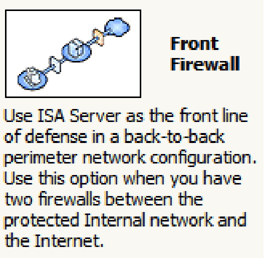
3-Leg Perimeter

Connect your Internal network to the Internet, protect it from intruders, and publish services to the Internet from a Perimeter network.

Figure 4: ISA Server 2006 – 3-leg Perimeter network template

Front Firewall

The Front Firewall template assumes that ISA Server is in Front of another Firewall directly on the Edge of the network. The place between the Front Firewall and the Back Firewall can be used as the Perimeter network or DMZ.



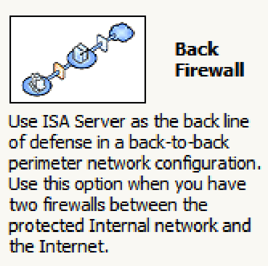
Front Firewall

Use ISA Server as the front line of defense in a back-to-back perimeter network configuration. Use this option when you have two firewalls between the protected Internal network and the Internet.

Figure 5: ISA Server 2006 – Front Firewall network template

Back Firewall

The Back Firewall template can be used by ISA Server Administrators, when ISA Server is placed behind a Front Firewall. The Back firewall protects the Internal network from access from the DMZ and the external network and it controls the network traffic which is allowed from DMZ hosts and from the Front Firewall.



Back Firewall

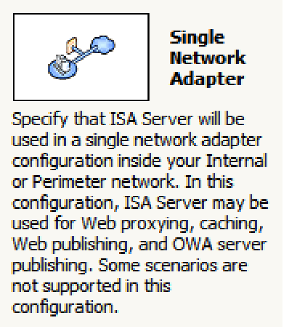
Use ISA Server as the back line of defense in a back-to-back perimeter network configuration. Use this option when you have two firewalls between the protected Internal network and the Internet.

Figure 6: ISA Server 2006 – Back Firewall network template

Single Network Adapter

The Single Network Adapter template has some limitations, because a ISA Server with only one network interface cannot be used as a real Firewall, so many services are not available. Only the following features are available:

- Forward Web Proxy requests that use HTTP, Secure HTTP (HTTPS), or File Transfer Protocol (FTP) for downloads
- Cache Web content for use by clients on the corporate network
- Web publishing to help protect published Web or FTP servers
- Microsoft Outlook Web Access, ActiveSync, and remote procedure call (RPC) over HTTP publishing



Single Network Adapter

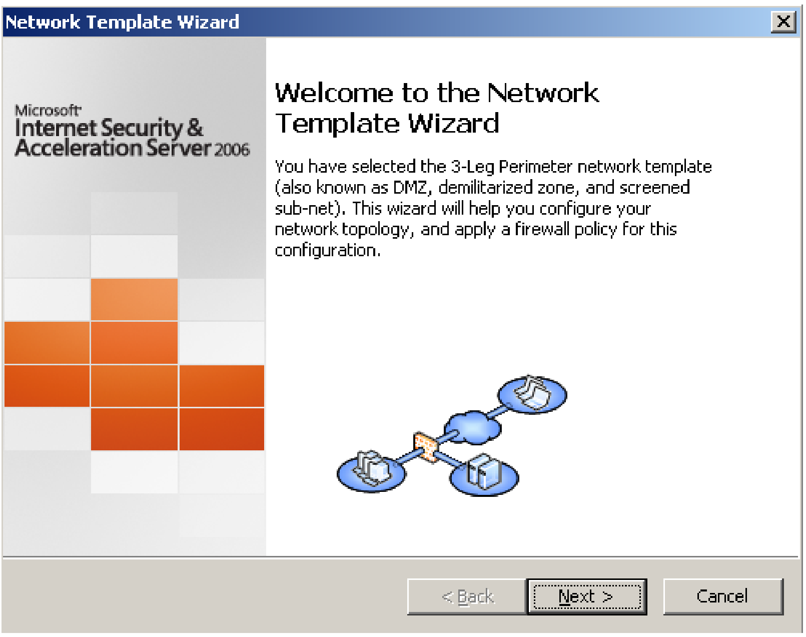
Specify that ISA Server will be used in a single network adapter configuration inside your Internal or Perimeter network. In this configuration, ISA Server may be used for Web proxying, caching, Web publishing, and OWA server publishing. Some scenarios are not supported in this configuration.

Figure 7: ISA Server 2006 – Single Network Adapter network template

Using the Network Template Wizard

ISA Server 2006 offers a Network Template Wizard which can be used to configure the network topology with networks, network rules and Firewall rules.

In the Task Pane select the required network template.



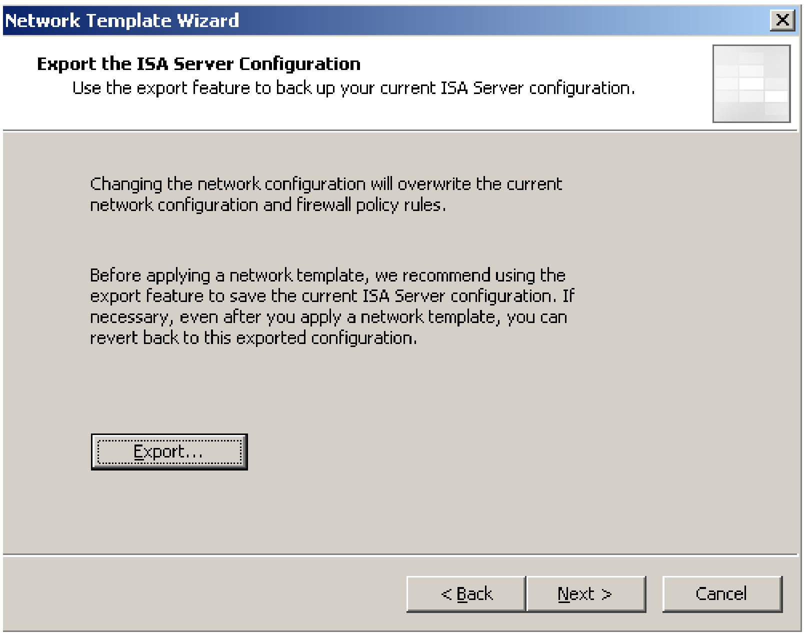
Network Template Wizard

Welcome to the Network Template Wizard

You have selected the 3-Leg Perimeter network template (also known as DMZ, demilitarized zone, and screened sub-net). This wizard will help you configure your network topology, and apply a firewall policy for this configuration.

Figure 8: Network Template Wizard

The Wizard will guide you through the entire process. As a first step you should export your current ISA Server configuration as a failback method, because the Wizard will overwrite the current network configuration and Firewall policy rules, except the System policy rules.



Network Template Wizard

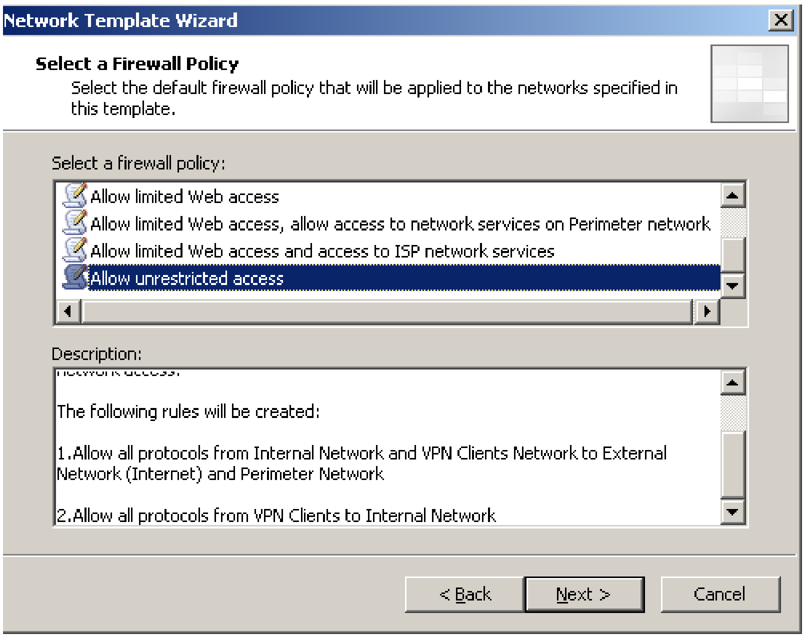
Export the ISA Server Configuration
Use the export feature to back up your current ISA Server configuration.

Changing the network configuration will overwrite the current network configuration and firewall policy rules.

Before applying a network template, we recommend using the export feature to save the current ISA Server configuration. If necessary, even after you apply a network template, you can revert back to this exported configuration.

Figure 9: Export the ISA Server Configuration

As a next step you have to define the Internal Network IP addresses. After that, you have to choice a predefined Firewall Policy. You should NOT select the Firewall Policy – *Allow unrestricted access* – because this rule allows all outgoing network traffic.



Network Template Wizard

Select a Firewall Policy

Select the default firewall policy that will be applied to the networks specified in this template.

Select a firewall policy:

- Allow limited Web access
- Allow limited Web access, allow access to network services on Perimeter network
- Allow limited Web access and access to ISP network services
- Allow unrestricted access

Description:

network access.

The following rules will be created:

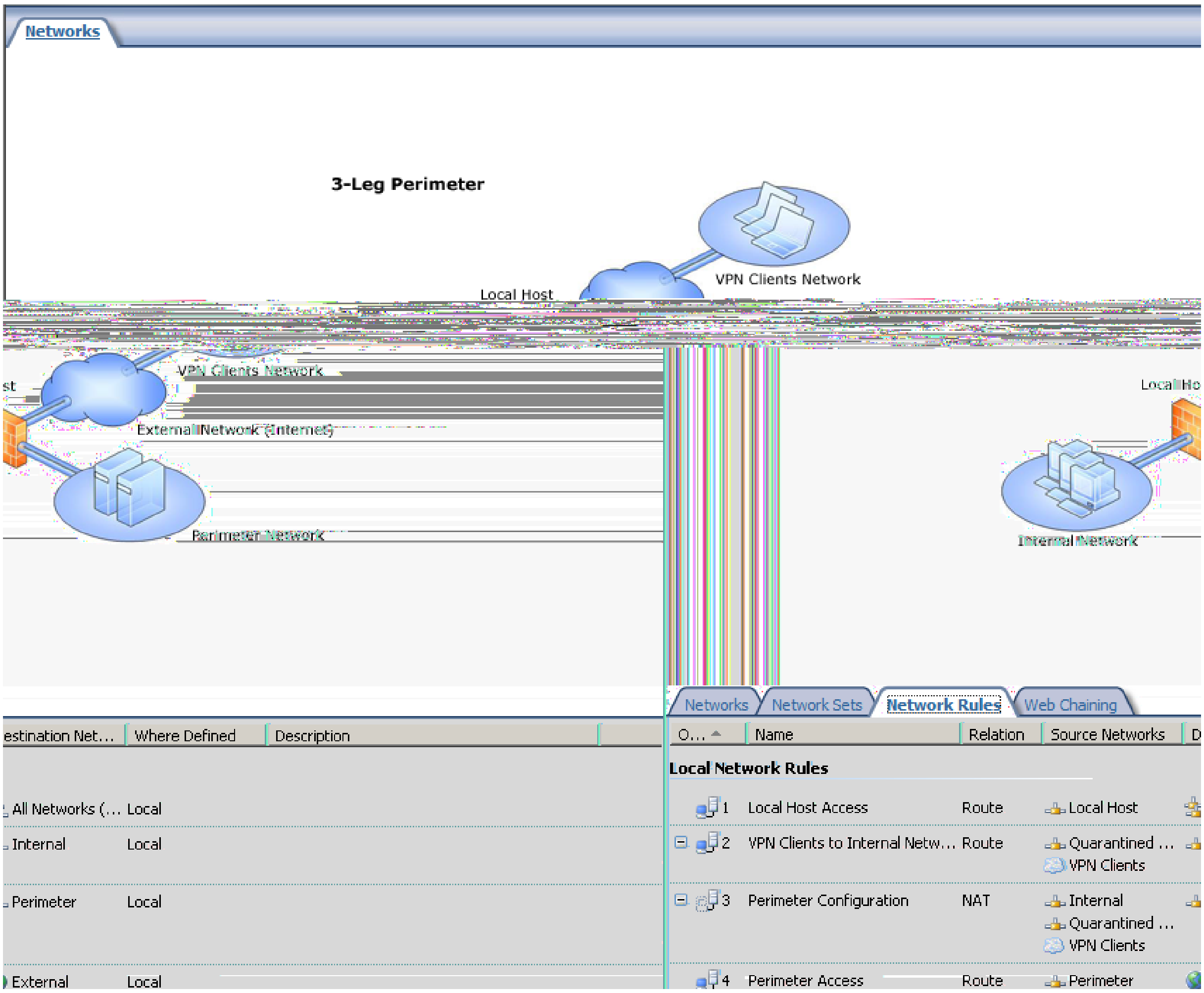
1.Allow all protocols from Internal Network and VPN Clients Network to External Network (Internet) and Perimeter Network

2.Allow all protocols from VPN Clients to Internal Network

Figure 10: Select a Firewall Policy

Attention: After the Network Rule Template Wizard has finished, you should modify the created Firewall rule to an absolute allowed minimum. A Firewall should always have a rule set with a minimum of allowed connections.

After the Wizard has finished, you can see the results in the *Configuration – Networks* tab.



estination Net...	Where Defined	Description
All Networks (...	Local	
Internal	Local	
Perimeter	Local	
External	Local	

O...	Name	Relation	Source Networks	D
Local Network Rules				
1	Local Host Access	Route	Local Host	
2	VPN Clients to Internal Netw...	Route	Quarantined ... VPN Clients	
3	Perimeter Configuration	NAT	Internal Quarantined ... VPN Clients	
4	Perimeter Access	Route	Perimeter	

Figure 11: ISA Server Network rules

The Wizard creates a network rule relationship from type NAT between the Internal and the Perimeter network and a Route relationship between the Perimeter network and the external network. You have to change this if your Servers in the Perimeter network contain private IP addresses.

Customizing Network Templates

It is possible to customize the predefined Network Template graphics to extend it with your own information like Server names or your own customized topology.
Network templates consist of two components:

- An XML file pro network template
- A Bitmap graphic pro network template

The XML file contains information about the necessary settings to create the required network, network rules and Firewall rule objects. The bitmap is only a graphic which shows the selected network template. You can find the XML and BMP file in the following directory: \Program Files\Microsoft ISA Server\NetworkTemplates.

It is possible to edit the bitmap files via Microsoft Paint or any other related program as you can see in the following picture.

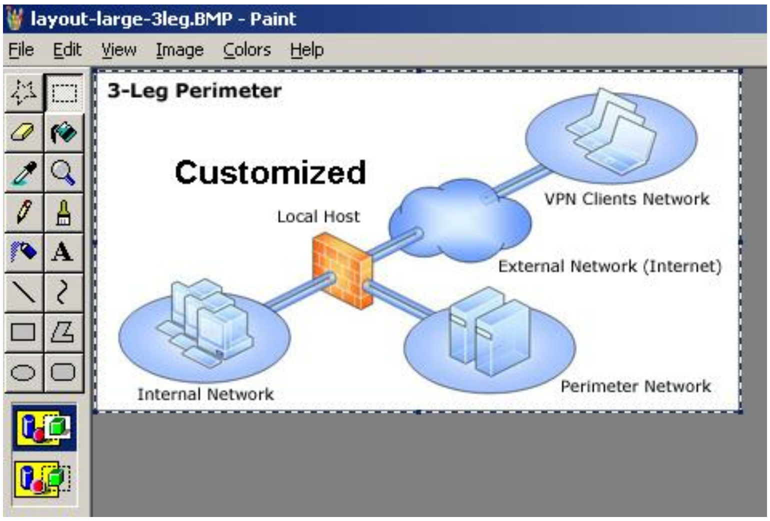
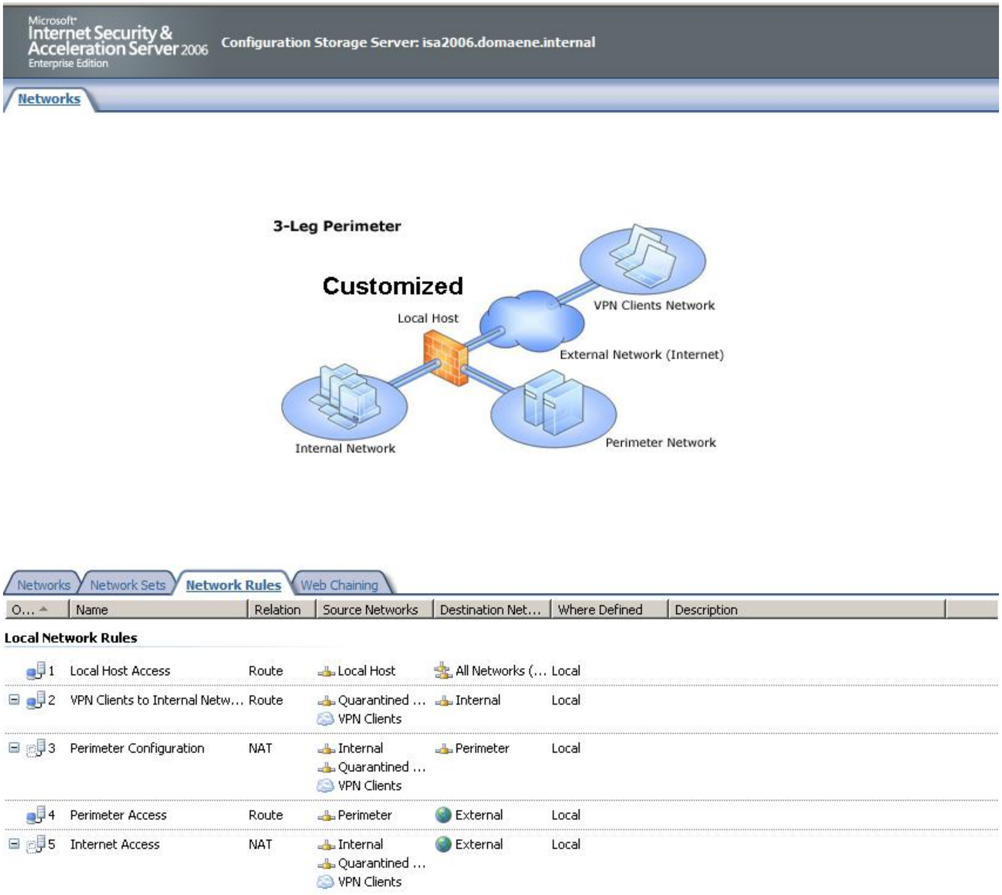

layout-large-3leg.BMP - Paint
File Edit View Image Colors Help
3-Leg Perimeter
Customized
Local Host
VPN Clients Network
External Network (Internet)
Internal Network
Perimeter Network

Figure 12: Customize the Network templates with Microsoft Paint

After you modified the template, you will see the changes in the ISA MMC.
Attention: It may be possible that you must refresh the view or to close and reopen the ISA MMC to see the changes.


Microsoft Internet Security & Acceleration Server 2006 Enterprise Edition
Configuration Storage Server: isa2006.domaene.internal
Networks
3-Leg Perimeter
Customized
Local Host
VPN Clients Network
External Network (Internet)
Internal Network
Perimeter Network
Networks
Network Sets
Network Rules
Web Chaining

Local Network Rules

O…	Name	Relation	Source Networks	Destination Net…	Where Defined	Description
1	Local Host Access	Route	Local Host	All Networks (…	Local	
2	VPN Clients to Internal Netw…	Route	Quarantined … VPN Clients	Internal	Local	
3	Perimeter Configuration	NAT	Internal Quarantined … VPN Clients	Perimeter	Local	
4	Perimeter Access	Route	Perimeter	External	Local	
5	Internet Access	NAT	Internal Quarantined … VPN Clients	External	Local	

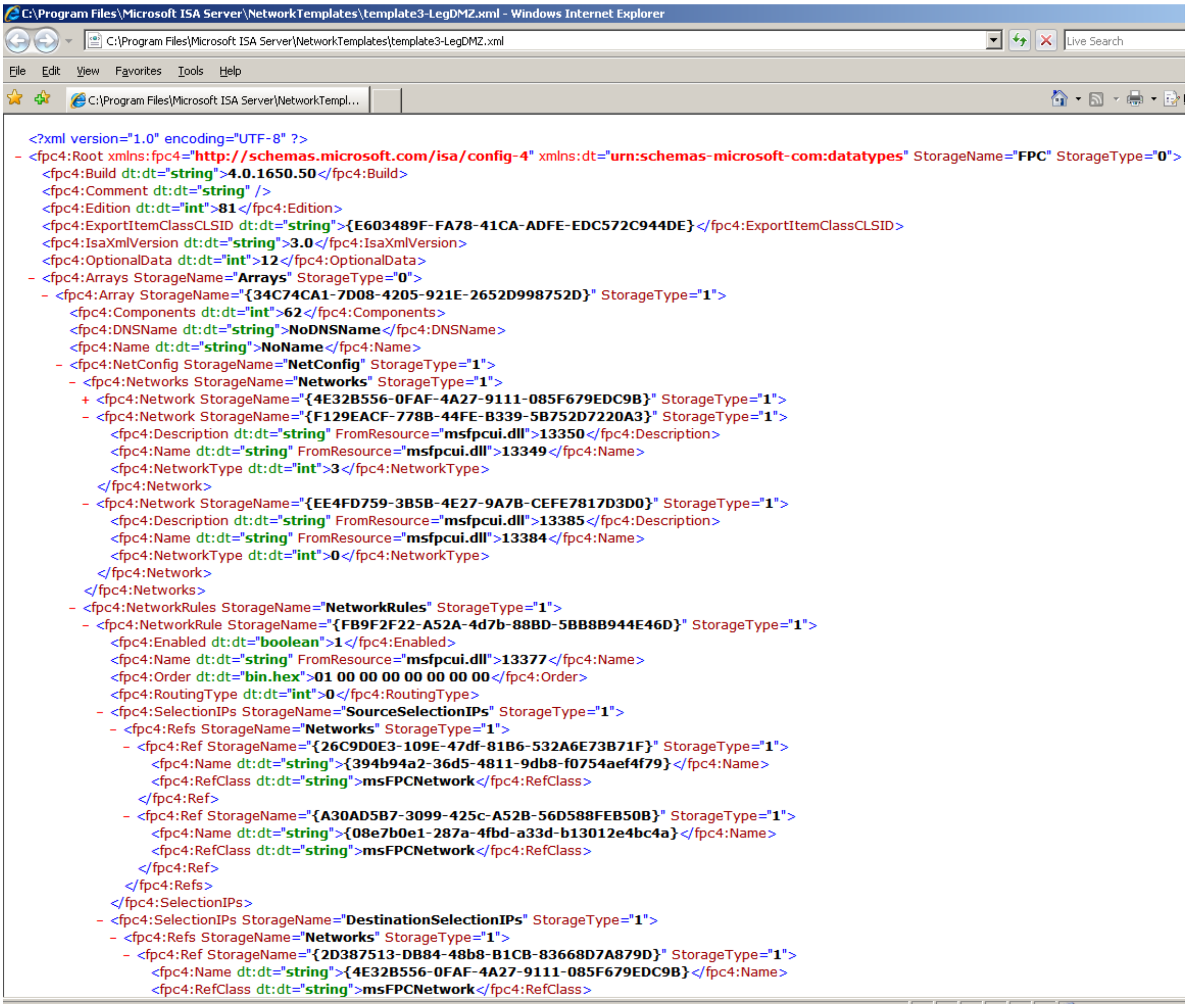
Figure 13: Customized Network Template

The XML template files

The XML file contains information about the necessary settings to create the required network, network rules and Firewall rule objects. The network templates are defined

in the ISA object called FPCNetworkTemplate. The FPCNetworkTemplate object allows you to set a name and description for the network template.
The XML file that contains a network template configuration includes:

- Networks and network sets
- Network rules that describe the relationships between various networks and network sets
- Policy elements
- Policies


C:\Program Files\Microsoft ISA Server\NetworkTemplates\template3-LegDMZ.xml - Windows Internet Explorer
C:\Program Files\Microsoft ISA Server\NetworkTemplates\template3-LegDMZ.xml
Live Search
File
Edit
View
Favorites
Tools
Help
C:\Program Files\Microsoft ISA Server\NetworkTempl...

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <fpc4:Root xmlns:fpc4="http://schemas.microsoft.com/isa/config-4" xmlns:dt="urn:schemas-microsoft-com:datatypes" StorageName="FPC" StorageType="0">
    <fpc4:Build dt:dt="string">4.0.1650.50</fpc4:Build>
    <fpc4:Comment dt:dt="string" />
    <fpc4:Edition dt:dt="int">81</fpc4:Edition>
    <fpc4:ExportItemClassCLSID dt:dt="string">{E603489F-FA78-41CA-ADFE-EDC572C944DE}</fpc4:ExportItemClassCLSID>
    <fpc4:IsaXmlVersion dt:dt="string">3.0</fpc4:IsaXmlVersion>
    <fpc4:OptionalData dt:dt="int">12</fpc4:OptionalData>
  - <fpc4:Arrays StorageName="Arrays" StorageType="0">
    - <fpc4:Array StorageName="{34C74CA1-7D08-4205-921E-2652D998752D}" StorageType="1">
        <fpc4:Components dt:dt="int">62</fpc4:Components>
        <fpc4:DNSName dt:dt="string">NoDNSName</fpc4:DNSName>
        <fpc4:Name dt:dt="string">NoName</fpc4:Name>
      - <fpc4:NetConfig StorageName="NetConfig" StorageType="1">
        - <fpc4:Networks StorageName="Networks" StorageType="1">
          + <fpc4:Network StorageName="{4E32B556-0FAF-4A27-9111-085F679EDC9B}" StorageType="1">
          - <fpc4:Network StorageName="{F129EACF-778B-44FE-B339-5B752D7220A3}" StorageType="1">
              <fpc4:Description dt:dt="string" FromResource="msfpcui.dll">13350</fpc4:Description>
              <fpc4:Name dt:dt="string" FromResource="msfpcui.dll">13349</fpc4:Name>
              <fpc4:NetworkType dt:dt="int">3</fpc4:NetworkType>
            </fpc4:Network>
          - <fpc4:Network StorageName="{EE4FD759-3B5B-4E27-9A7B-CEFE7817D3D0}" StorageType="1">
              <fpc4:Description dt:dt="string" FromResource="msfpcui.dll">13385</fpc4:Description>
              <fpc4:Name dt:dt="string" FromResource="msfpcui.dll">13384</fpc4:Name>
              <fpc4:NetworkType dt:dt="int">0</fpc4:NetworkType>
            </fpc4:Network>
          </fpc4:Networks>
        - <fpc4:NetworkRules StorageName="NetworkRules" StorageType="1">
          - <fpc4:NetworkRule StorageName="{FB9F2F22-A52A-4d7b-88BD-5BB8B944E46D}" StorageType="1">
              <fpc4:Enabled dt:dt="boolean">1</fpc4:Enabled>
              <fpc4:Name dt:dt="string" FromResource="msfpcui.dll">13377</fpc4:Name>
              <fpc4:Order dt:dt="bin.hex">01 00 00 00 00 00 00 00</fpc4:Order>
              <fpc4:RoutingType dt:dt="int">0</fpc4:RoutingType>
            - <fpc4:SelectionIPs StorageName="SourceSelectionIPs" StorageType="1">
              - <fpc4:Refs StorageName="Networks" StorageType="1">
                - <fpc4:Ref StorageName="{26C9D0E3-109E-47df-81B6-532A6E73B71F}" StorageType="1">
                    <fpc4:Name dt:dt="string">{394b94a2-36d5-4811-9db8-f0754aef4f79}</fpc4:Name>
                    <fpc4:RefClass dt:dt="string">msFPCNetwork</fpc4:RefClass>
                  </fpc4:Ref>
                - <fpc4:Ref StorageName="{A30AD5B7-3099-425c-A52B-56D588FEB50B}" StorageType="1">
                    <fpc4:Name dt:dt="string">{08e7b0e1-287a-4fbd-a33d-b13012e4bc4a}</fpc4:Name>
                    <fpc4:RefClass dt:dt="string">msFPCNetwork</fpc4:RefClass>
                  </fpc4:Ref>
                </fpc4:Refs>
              </fpc4:SelectionIPs>
            - <fpc4:SelectionIPs StorageName="DestinationSelectionIPs" StorageType="1">
              - <fpc4:Refs StorageName="Networks" StorageType="1">
                - <fpc4:Ref StorageName="{2D387513-DB84-48b8-B1CB-83668D7A879D}" StorageType="1">
                    <fpc4:Name dt:dt="string">{4E32B556-0FAF-4A27-9111-085F679EDC9B}</fpc4:Name>
                    <fpc4:RefClass dt:dt="string">msFPCNetwork</fpc4:RefClass>
```

Figure 14: 3-Leg DMZ – XML Template

Conclusion

In this article, I tried to give you all information that is necessary to build your own secure network infrastructure with ISA Server 2006. I also showed you how to customize the network template bitmaps. In my opinion, network templates are a good starting point for ISA beginners, but if you are an experienced ISA Server Administrator, you should build your own infrastructure by modifying the ISA Server networks, network rules and Firewall policies manually.

Related links

Network Concepts in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794774.aspx

Using ISA Server 2004 Network Templates to Automatically Create Access Policy: The Edge Firewall Template
http://www.isaserver.org/tutorials/2004edgefirewall.html
Configuring ISA Server 2004 on a Computer with a Single Network Adapter
http://technet.microsoft.com/en-us/library/cc302586.aspx
Troubleshooting Network Configuration in ISA Server 2004
http://technet.microsoft.com/de-de/library/cc302656(en-us).aspx
Configuring ISA Server 2004 on a Computer with a Single Network Adapter
http://technet.microsoft.com/en-us/library/cc302586.aspx
The features and limitations of a single-homed ISA Server 2006, ISA Server 2004, or Microsoft Forefront Threat Management Gateway, Medium Business Edition computer
http://support.microsoft.com/default.aspx?scid=kb;en-us;838364
FPCNetworkTemplate
http://msdn.microsoft.com/en-us/library/aa491423.aspx