


Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

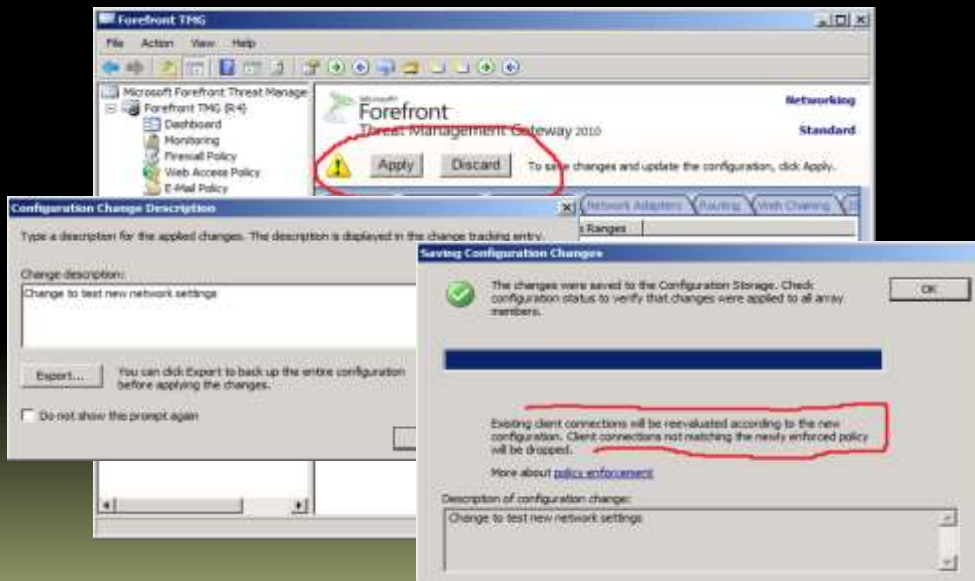
MULTI-NETWORKING AND BASIC CONFIGURATION



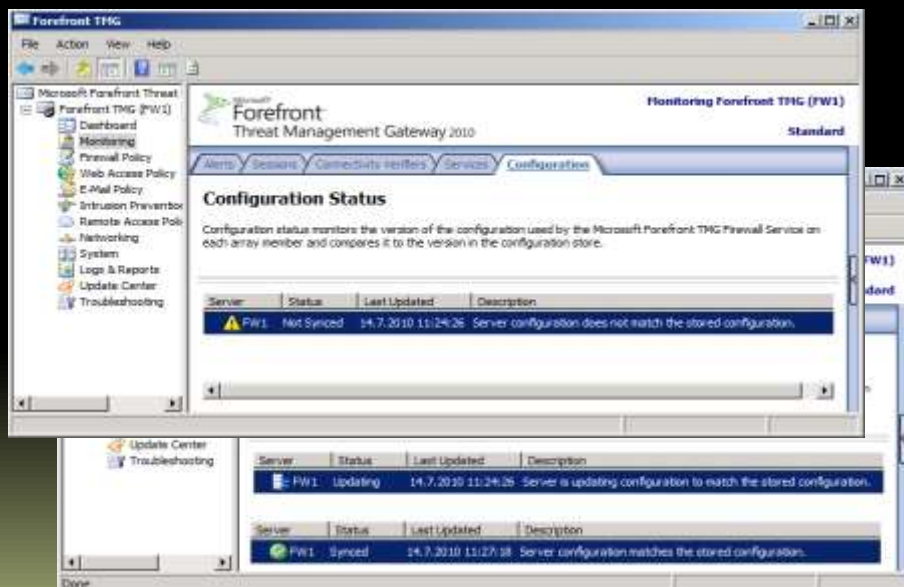
Threat Management Gateway 2010

BASIC CONFIGURATION

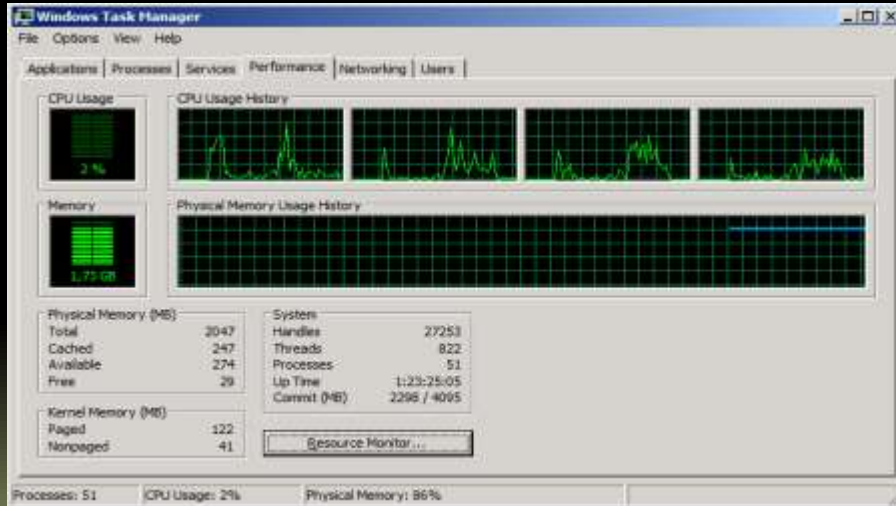
Configuration changes



Waiting for application



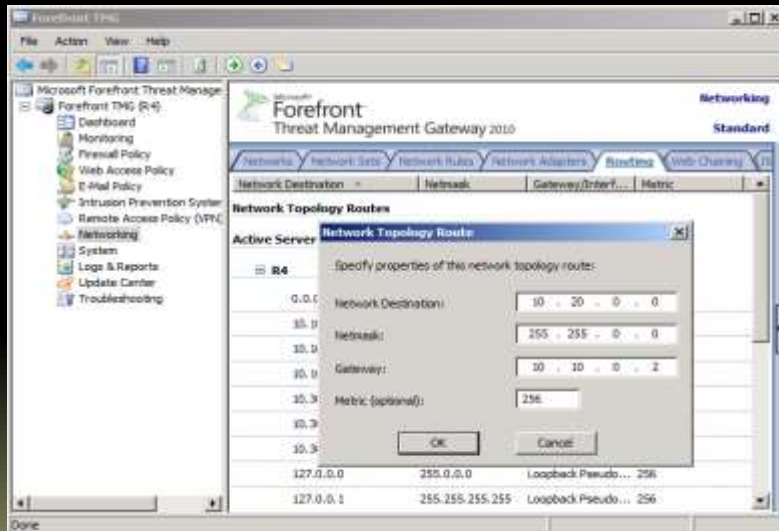
Waiting for application



New NIC and routing GUI



New NIC and routing GUI



Lab

- Add all public addresses to the **Internet** interface of **FW₁**
 - 81.0.0.178-182 / 255.255.255.248
- Check that the route to **10.20.x.x** network already exists
 - **route print**
- Remove the route by using **route delete** and recreate it by using the TMG user interface

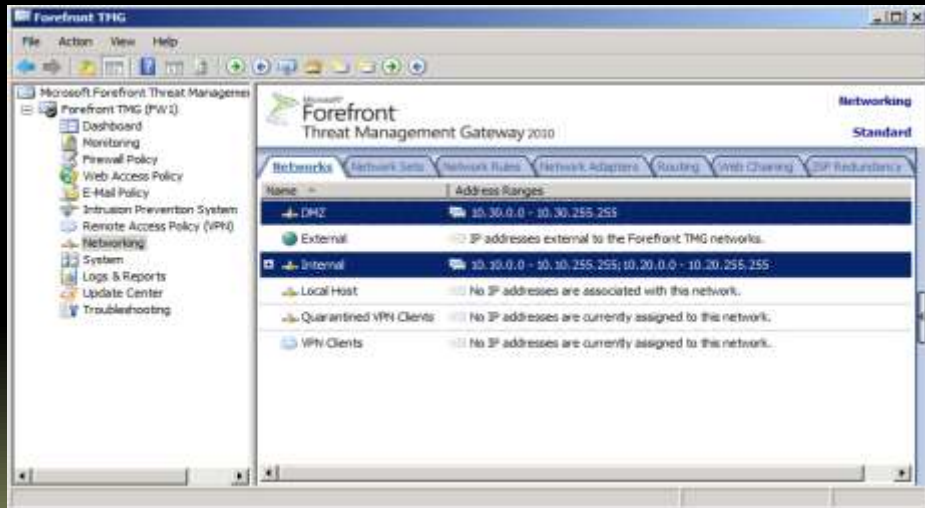
Threat Management Gateway 2010

MULTI-NETWORKING

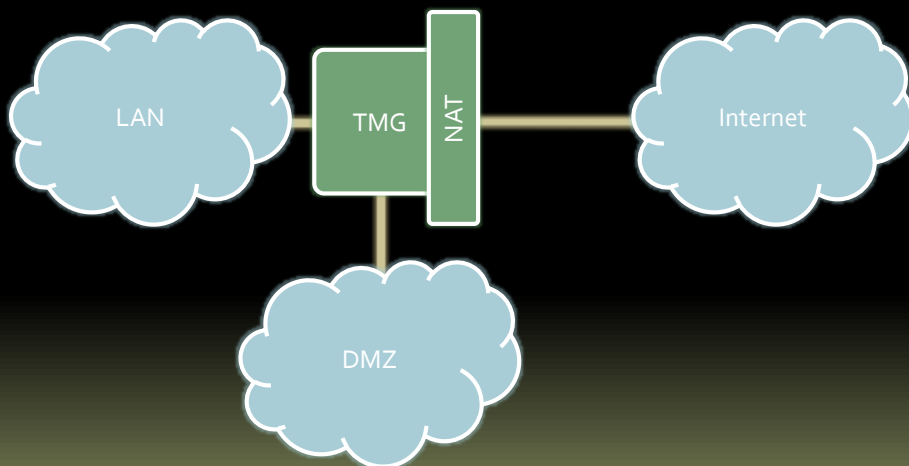
Network

- IP range used in rules
- Network adapter identified and paired by its IP address
- One-to-one mapping
 - consider more IP addresses

Networks



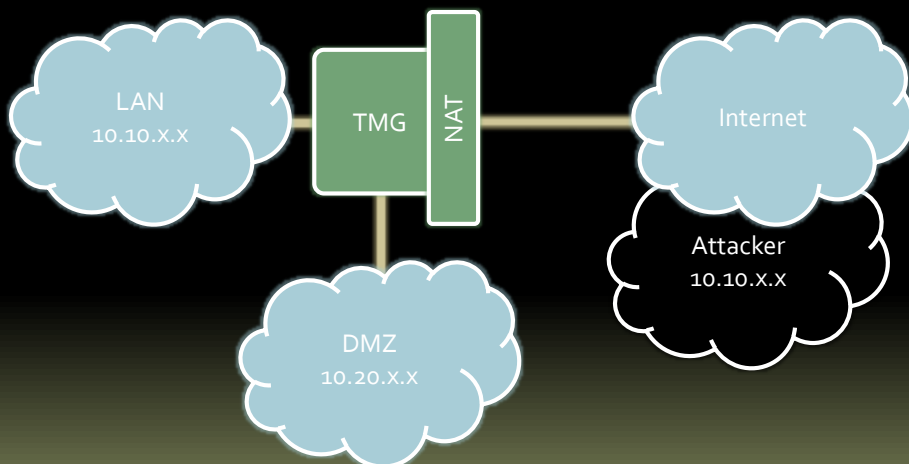
Example networking



IP anti-spoofing

- Packets received on an interface must be from the defined IP range
 - or discarded
- Packets received on the **External** interface must **not be** from any other defined range
 - or discarded

IP anti-spoofing



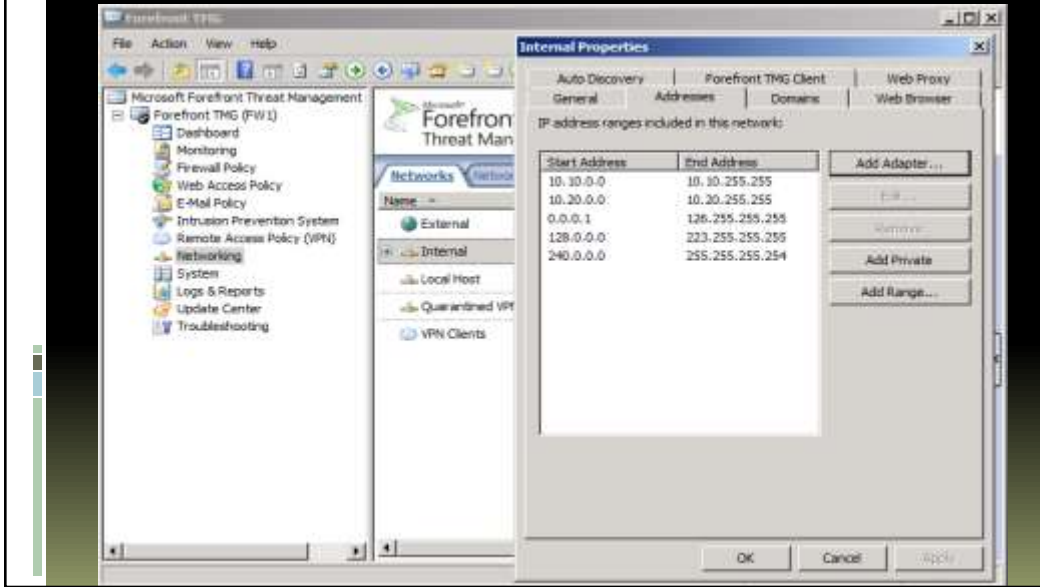
Network templates

- Internal
 - member of **All Protected Networks** network set
 - **Web Proxy enabled** on TCP 8080
- Perimeter
 - member of **All Protected Networks** network set
 - **Web Proxy not enabled**
- External
 - **exempt** from **All Protected Networks** network set
 - **Web Proxy not enabled**

Lab

- Reset all actual **alerts**
- Try removing the **10.20.x.x** network from **Internal** network object
- Note the **Configuration error** alert
- Move **Seven1** computer into the **Brno** network and try
 - ping 10.30.0.21
- Note the **IP Spoofing** alert
- Repair the **Internal** network object configuration by adding its network adapter

Single NIC proxy



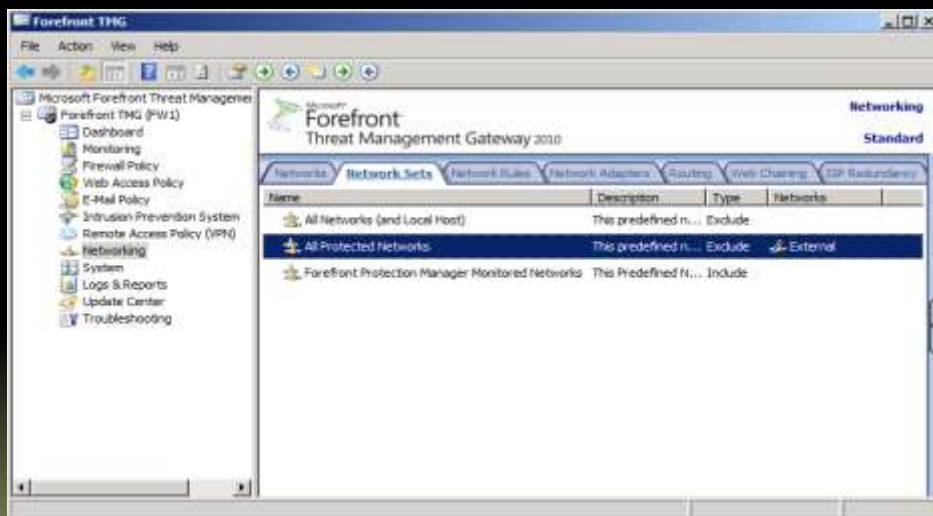
Threat Management Gateway 2010

NETWORK SETS

Network Sets

- Inclusive
- Exclusive
- Used to simplify rule configuration

Network Set



Threat Management Gateway 2010

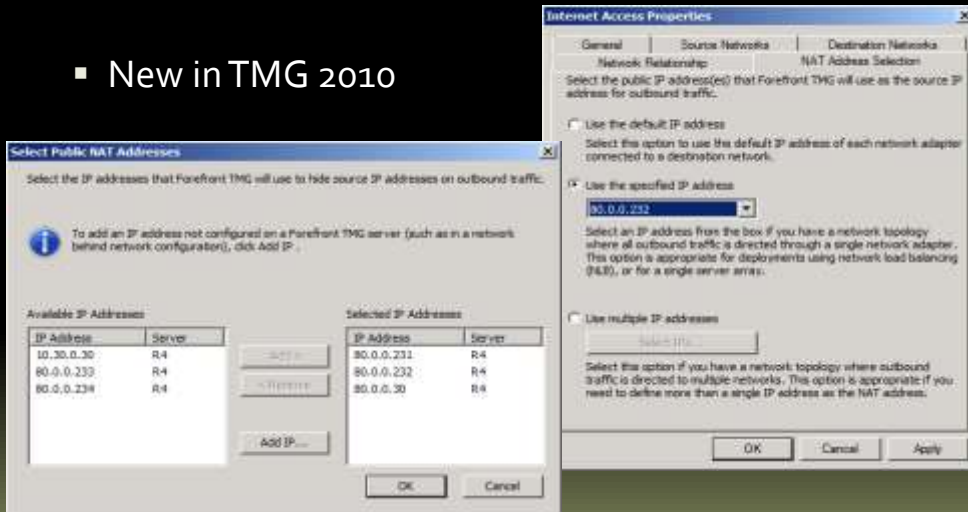
NETWORK RULES

Routing vs. NAT

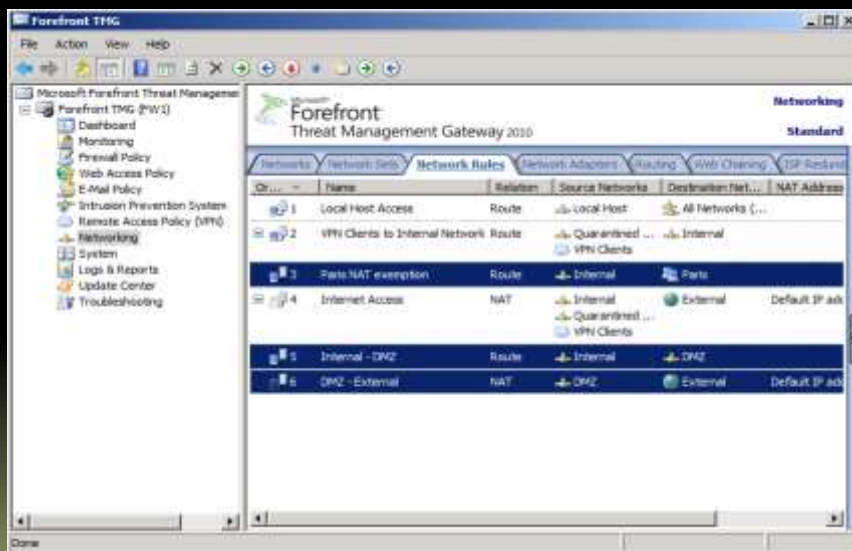
- **Network rule** must be present
 - or packets discarded
- Evaluated first when packet arrives
- **NAT** enables precise public IP setting
- **Network rules** are orderable
 - exempt some traffic from NAT

NAT public IP pool

- New in TMG 2010



Network Rules and Exemption



Lab

- Define new **DMZ** network object
- Define **route** relation from **Internal to DMZ**
- Define **NAT** relation from **DMZ to External**
- Define **NAT exemption** for the **10.50.x.x** range
 - define route relationship from Internal to 10.50.x.x

Threat Management Gateway 2010

ISP REDUNDANCY

ISP Redundancy

- For outbound connections only
 - require NAT relationship
- Load-balancing
 - used in a specific ration
 - all traffic, no filters per protocol etc.
- Failover
- Maximum of 2 NICs

ISP Redundancy

The screenshot displays the Microsoft Forefront Threat Management Gateway (TMG) 2010 console. The interface is titled "Forefront Threat Management Gateway 2010" and shows the "Networking" section. The "ISP Redundancy" tab is selected, displaying the "ISP Redundancy Model" set to "Failover only". A table lists the configured ISP connections:

ISP Connection	Gateway Address	Subnet Mask	Connectivity Detection	Role
Backup ISP	10.102.0.1	255.255.0.0	Enabled	Secondary
Internet	81.0.0.177	255.255.255.248	Enabled	Primary

Dead ISP detection

- Every **60 sec.** root DNS servers are polled
- The poll must fail for **3 times**
 - up to **2 minutes** before the ISP is switched

Failure detection

The screenshot displays the Microsoft Network Monitor 3.3 interface. The main window shows a list of captured frames. The selected frame (Frame 1279) is a TCP segment from source IP 81.0.0.178 to destination IP 198.32.64.12, port 12359 to port 53. The description indicates a SYN retransmit attempt for a DNS query.

Fr...	Time Offset	Source	Destination	Protocol Name	Description
1279	37.502579	81.0.0.178	198.32.64.12	TCP	TCP[Seq=2436276146, SrcPort=12359, DstPort=DNS(53), PayloadLen=0, Seq=2436276146, Win=0, Len=66]
1280	838.654296	30.102.10.82	192.33.4.12	TCP	TCP[Flags=.....S., SrcPort=12360, DstPort=DNS(53), PayloadLen=0, Seq=12360, Win=0, Len=66]
1281	838.661132	192.33.4.12	30.102.10.82	TCP	TCP[Flags=...A.S., SrcPort=DNS(53), DstPort=12360, PayloadLen=0, Seq=12360, Win=0, Len=66]
1282	838.662399	30.102.10.82	192.33.4.12	TCP	TCP[Flags=...A....., SrcPort=12360, DstPort=DNS(53), PayloadLen=0, Seq=12360, Win=0, Len=66]
1283	838.664062	30.102.10.82	192.33.4.12	TCP	TCP[Flags=...A.R., SrcPort=12360, DstPort=DNS(53), PayloadLen=0, Seq=12360, Win=0, Len=66]
1292	840.893554	81.0.0.178	198.32.64.12	TCP	TCP[SynRetransmit #1279]Flags=.....S., SrcPort=12359, DstPort=DNS(53), Seq=2436276146, Win=0, Len=66]
1303	846.933593	81.0.0.178	198.32.64.12	TCP	TCP[SynRetransmit #1279]Flags=.....S., SrcPort=12359, DstPort=DNS(53), Seq=2436276146, Win=0, Len=66]
1365	898.052734	81.0.0.178	202.12.27.33	TCP	TCP[Flags=.....S., SrcPort=12361, DstPort=DNS(53), PayloadLen=0, Seq=12361, Win=0, Len=66]
1366	898.830546	30.102.10.82	128.8.10.90	TCP	TCP[Flags=.....S., SrcPort=12362, DstPort=DNS(53), PayloadLen=0, Seq=12362, Win=0, Len=66]
1367	898.930664	128.8.10.90	30.102.10.82	TCP	TCP[Flags=...A.S., SrcPort=DNS(53), DstPort=12362, PayloadLen=0, Seq=12362, Win=0, Len=66]
1368	898.931640	30.102.10.82	128.8.10.90	TCP	TCP[Flags=...A....., SrcPort=12362, DstPort=DNS(53), PayloadLen=0, Seq=12362, Win=0, Len=66]

Frame Details:
Frame: Number = 1279, Captured Frame Length = 66, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-15-5D-0A-22-10], SourceAddress: [00-15-5D-0A-22-10]
IPv4: Src = 81.0.0.178, Dest = 198.32.64.12, Next Protocol = TCP, Packet ID = 22654, Total Length = 66
TCP: Flags=.....S., SrcPort=12359, DstPort=DNS(53), PayloadLen=0, Seq=2436276146, Ack=0, Win=0, Len=66

Failure detection

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) monitoring console. The interface includes a menu bar (File, Action, View, Help), a toolbar, and a left-hand navigation pane with categories like Dashboard, Monitoring, Firewall Policy, Web Access Policy, E-Mail Policy, Intrusion Prevention, Remote Access Policy, Networking, System, Logs & Reports, Update Center, and Troubleshooting. The main area is titled 'Monitoring Forefront TMG (FW1)' and 'Standard'. It features a tabbed interface with 'Alerts' selected. A table displays a list of alerts:

Alert	Latest	Status	Category
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 9:44:17	New	Firewall Service

Below the table, the 'Alert Information' section provides a description: 'Description: Connectivity to the Internet through ISP Internet cannot be established. Forefront TMG cannot connect to the ISP.'

Failure detection

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) monitoring console, similar to the first image. The interface and navigation pane are identical. The 'Alerts' tab is active, and the table displays a list of alerts:

Alert	Latest	Status	Category
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 9:44:17	New	Firewall Service

The 'Alert Information' section now shows a different description: 'Description: The ISP link Backup ISP is currently active.'

Network status dashboard

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) interface. The left-hand navigation pane lists various management areas: Dashboard, Monitoring, Firewall Policy, Web Access Policy, E-Mail Policy, Intrusion Prevention, Remote Access Policy, Networking, System, Logs & Reports, Update Center, and Troubleshooting. The main content area is titled "Forefront Threat Management Gateway 2010" and displays the "Dashboard" view. Under the "Alerts" section, there is a table with two entries: a Warning (1 new) and Information (1 new). Below this, the "Network Status" section shows a table of connectivity details.

Object	Status	Uptime	Bytes/Sec
Backup ISP	Internet	0d. 10h. 6m. 27s.	26
Internet	Local		
Connectivity verifiers	1		

Connectivity restored

This screenshot shows the "Alerts" console in the Forefront TMG interface. The "Alerts" tab is selected, and a list of events is displayed. The events are categorized by "ISP Redundancy" and include sub-entries for "Connection Unavailable", "Connection Active", and "Connections Available". The most recent event, "ISP Redundancy - Connections Available", is highlighted in blue. Below the list, the "Alert Information" section provides a description of the event.

Alert	Latest	Status	Category
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Unavailable	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 10:07:03	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 9:44:17	New	Firewall Service
ISP Redundancy - Connection Active	16.7.2010 10:07:03	New	Firewall Service
ISP Redundancy - Connections Available	16.7.2010 10:07:03	New	Firewall Service
ISP Redundancy - Connections Available	16.7.2010 10:07:03	New	Firewall Service

Alert Information
Description: Connectivity to the Internet through the ISP connections Internet and Backup ISP was restored.

Lab: Optional

- Enable ISP redundancy by using the Backup ISP (197.x.x.x) network interface
- Disable the Internet 81 network interface on R1 and wait for the TMG to detect the failure
- Monitor the failure by using TMG and reenables the original connectivity

Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

THANK YOU