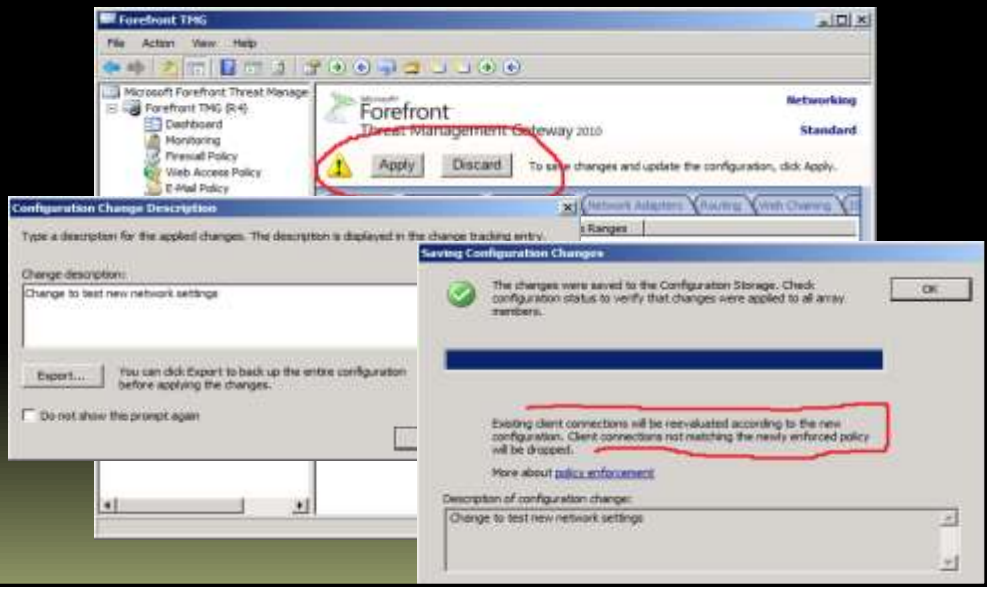
Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

MULTI-NETWORKING AND BASIC CONFIGURATION

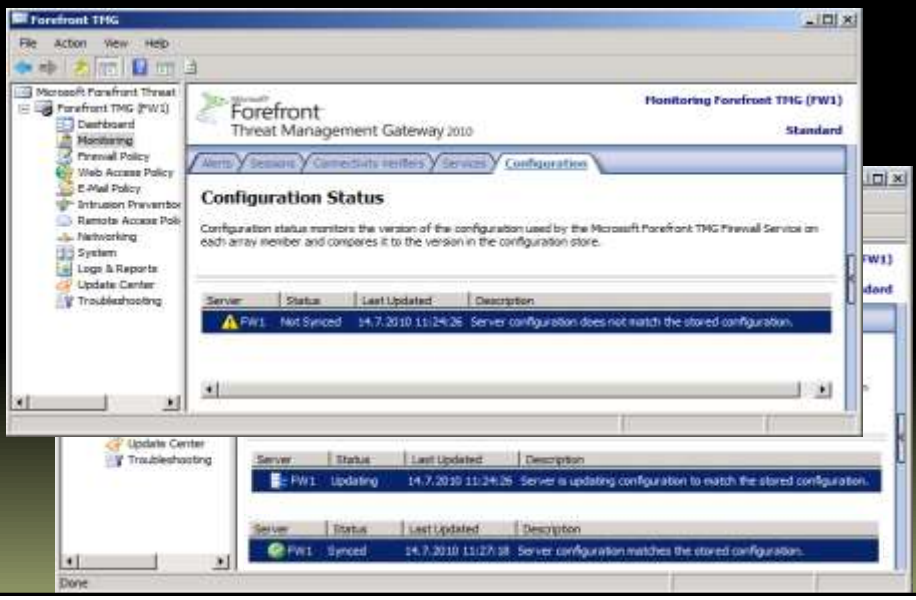
Threat Management Gateway 2010

BASIC CONFIGURATION

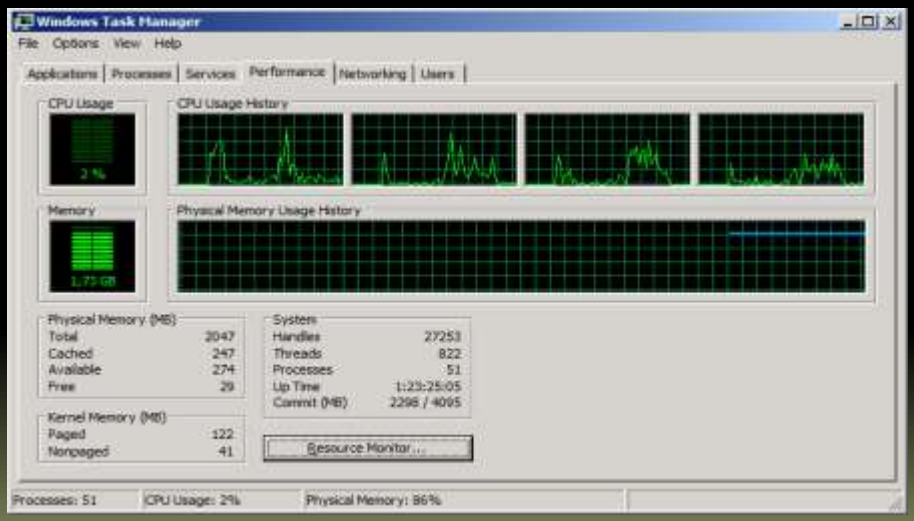
Configuration changes



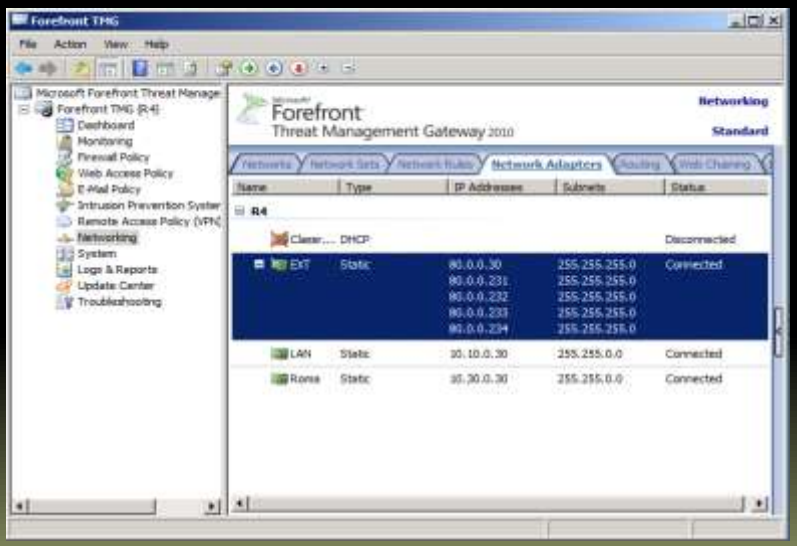
Waiting for application



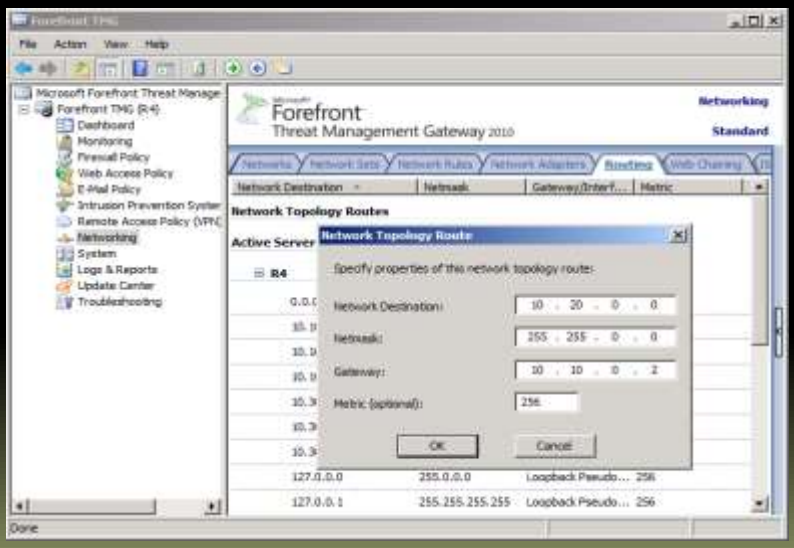
Waiting for application



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

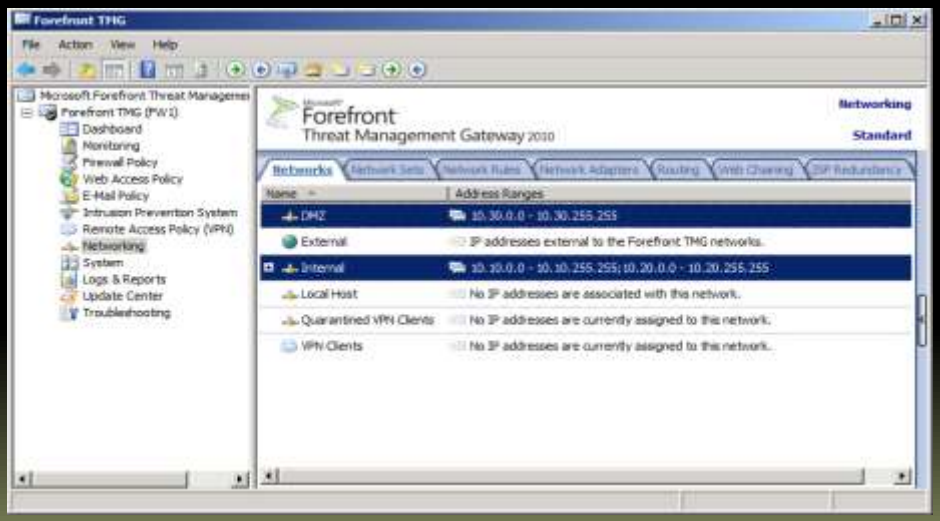
Threat Management Gateway 2010

MULTI-NETWORKING

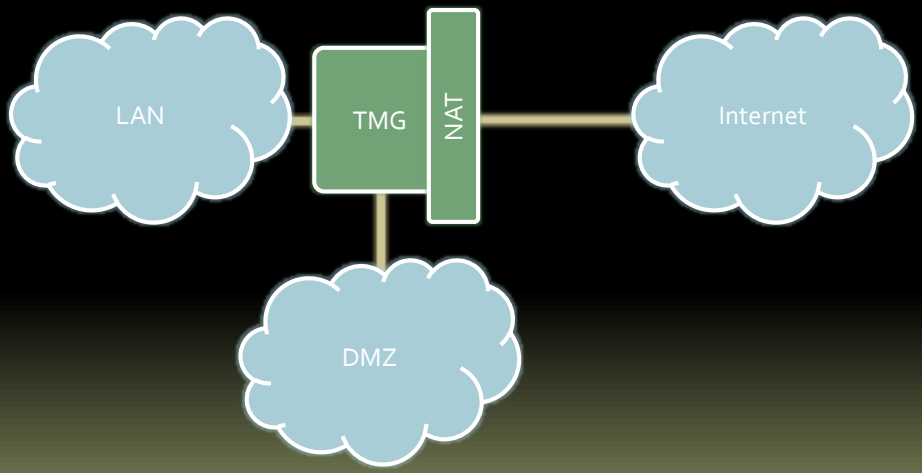
Network

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

Networks



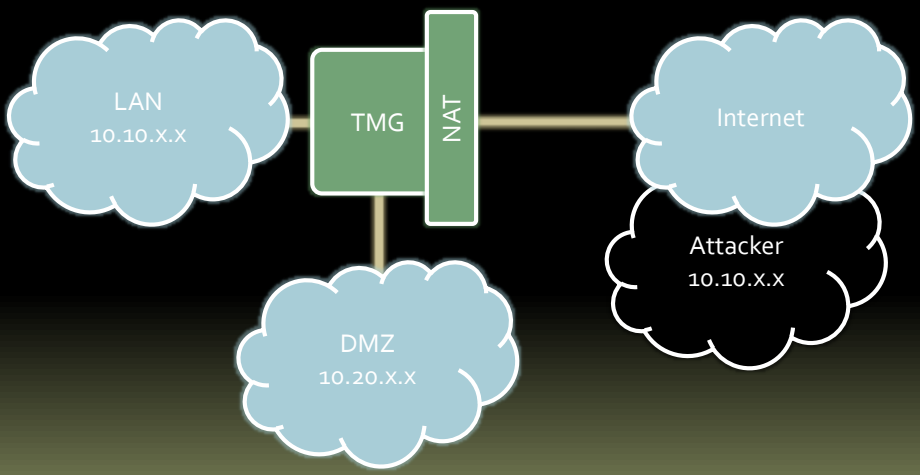
Example networking



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



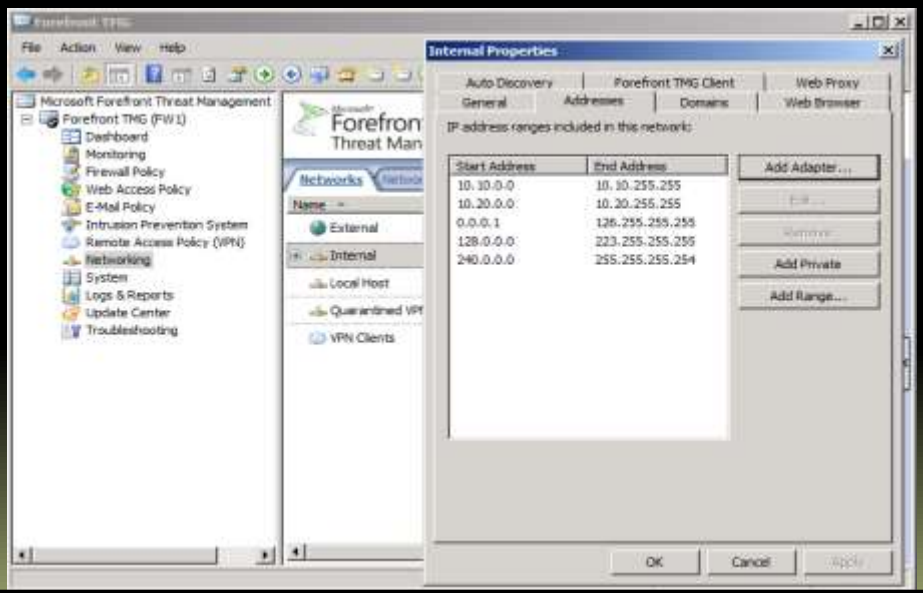
Network templates

- 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



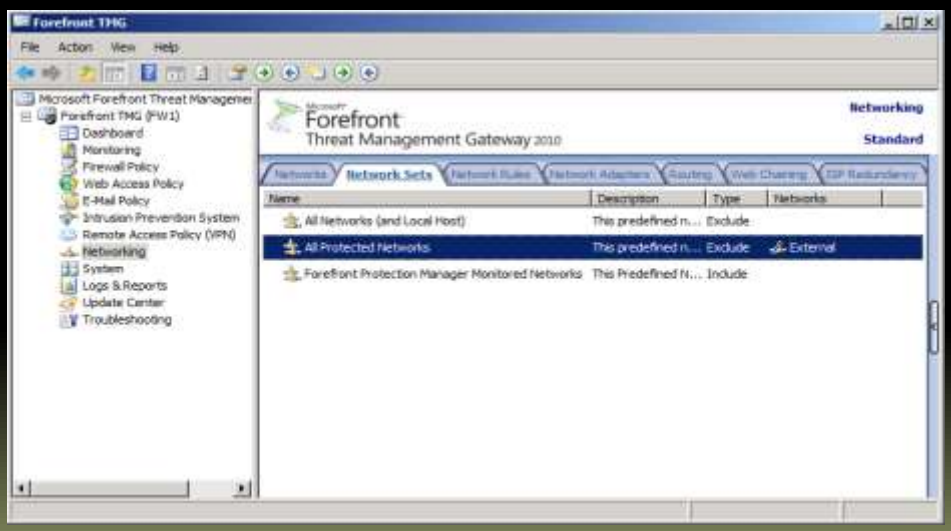
Threat Management Gateway 2010

NETWORK SETS

Network Sets

- Inclusive
- Exclusive
- Used to simplify rule configuration

Network Set



Threat Management Gateway 2010

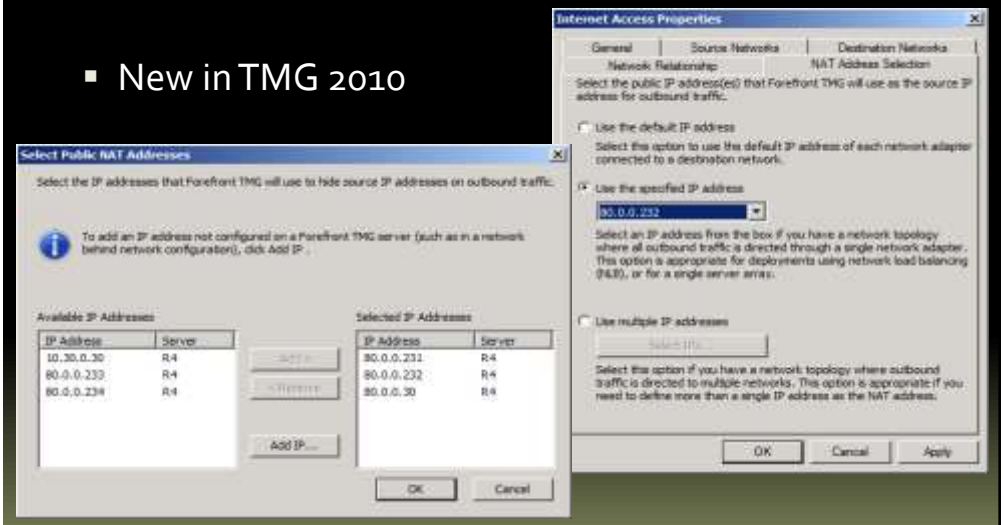
NETWORK RULES

Routing vs. NAT

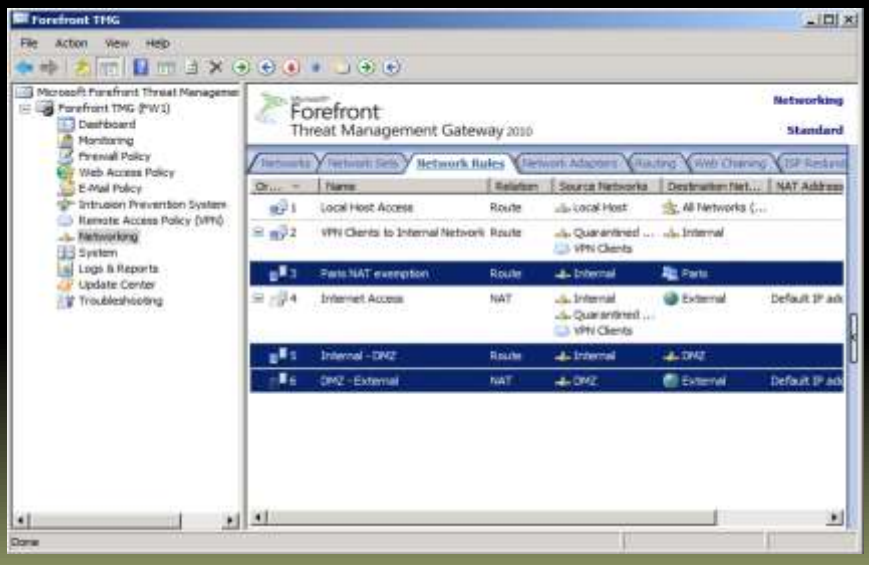
- Network rule must be present
  - or packets discarded
- Evaluated first when packet arrives
- NAT enables precise public IP setting
- Network rules are orderable
  - exempt some traffic from NAT

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

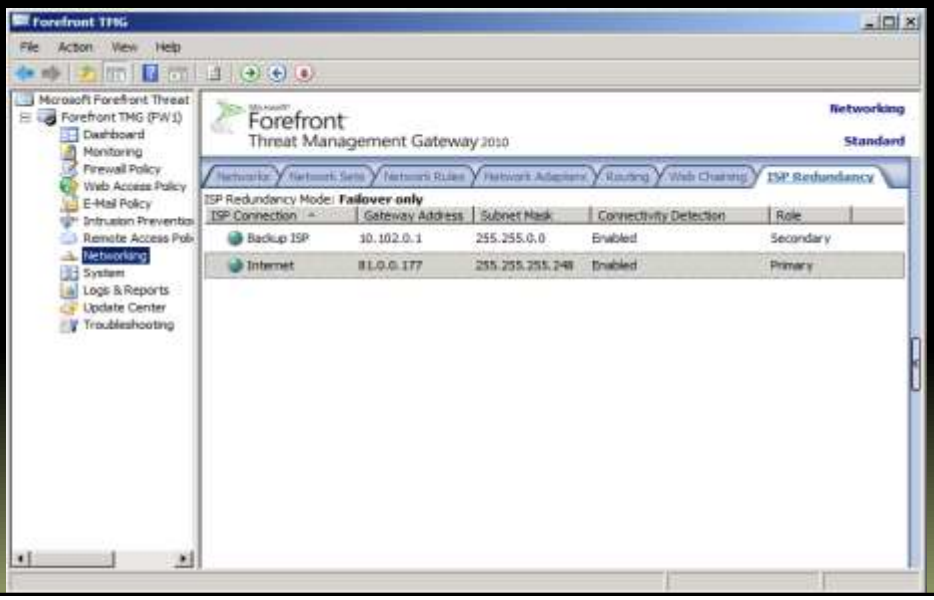
Threat Management Gateway 2010

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

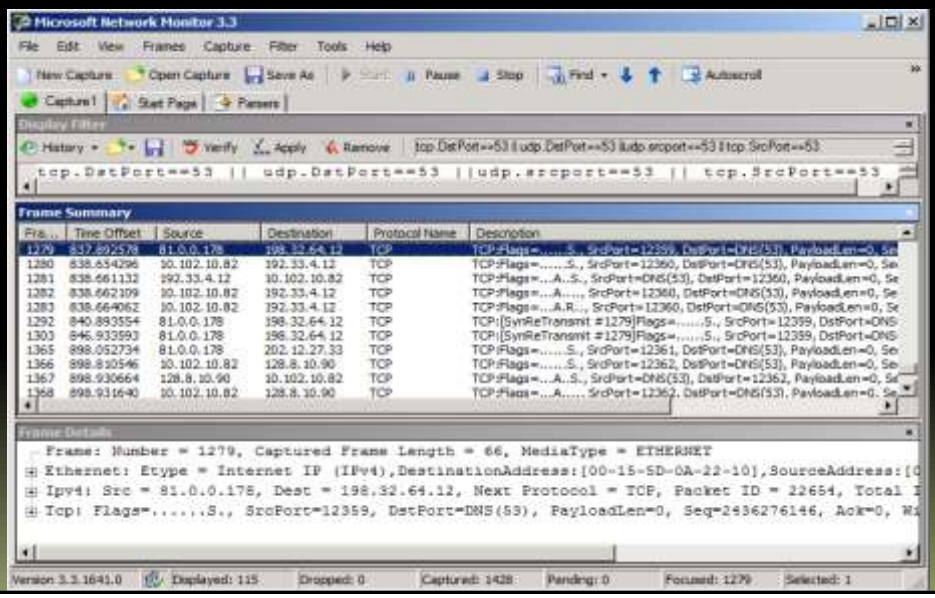
ISP Redundancy



Dead ISP detection

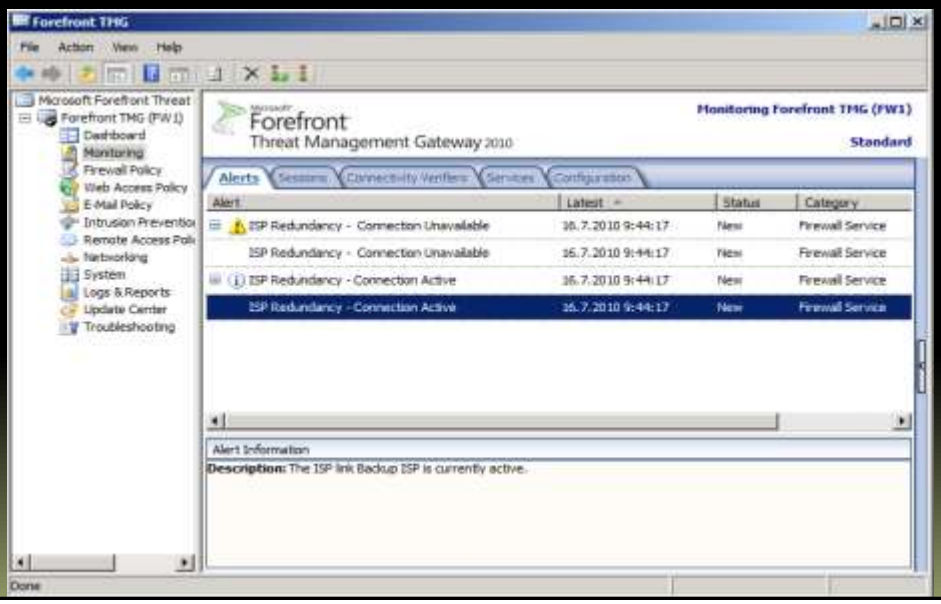
- Every 60 sec. root DNS servers are polled
- The poll must fail for 3 times
  - up to 2 minutes before the ISP is switched

Failure detection

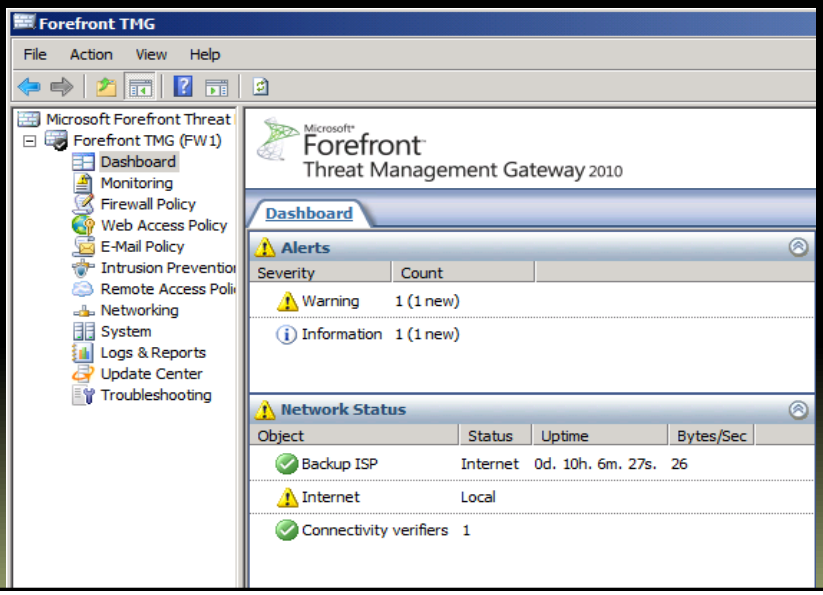


Failure detection

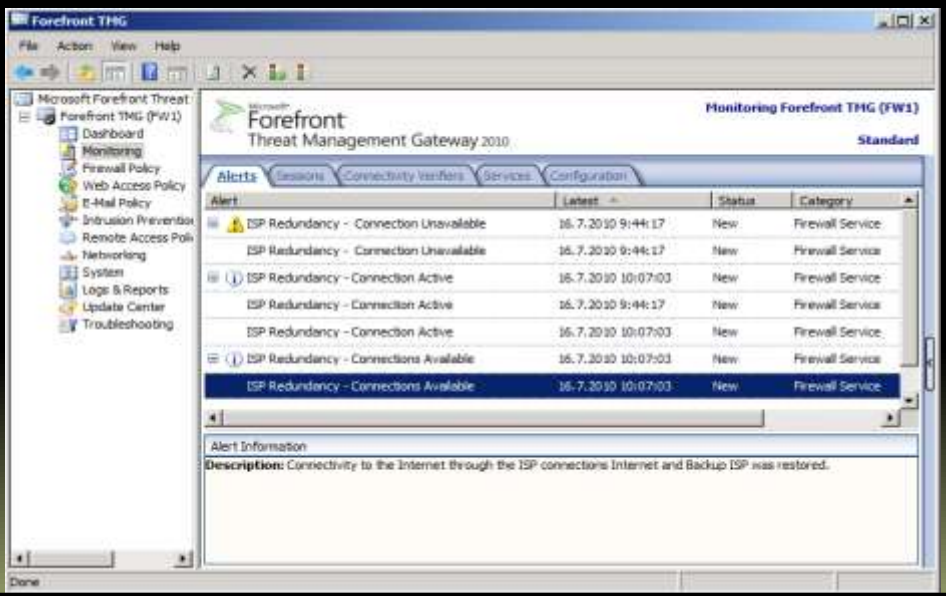
Failure detection



Network status dashboard



Connectivity 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 reenable the original connectivity

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

THANK YOU