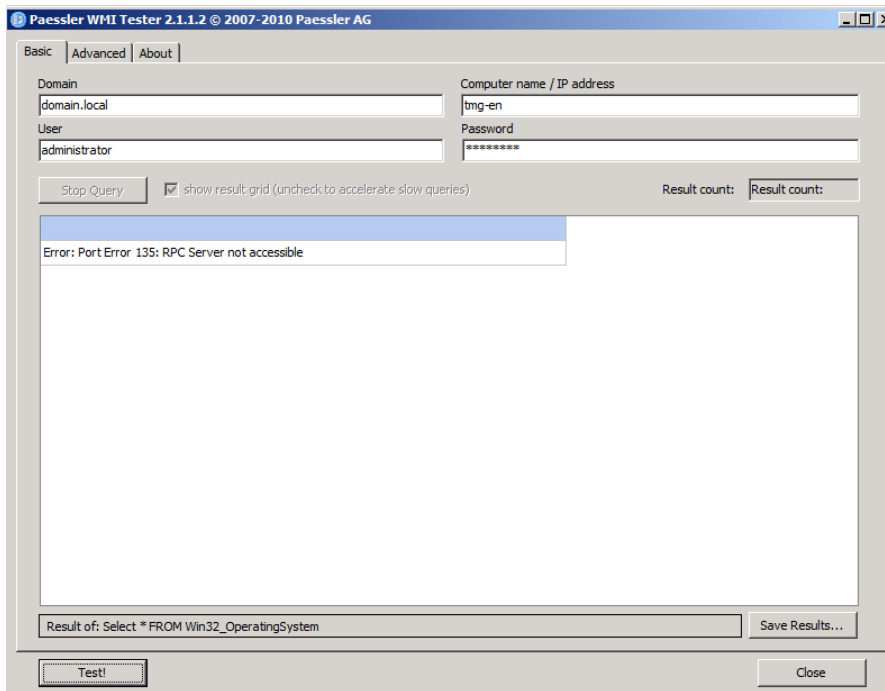
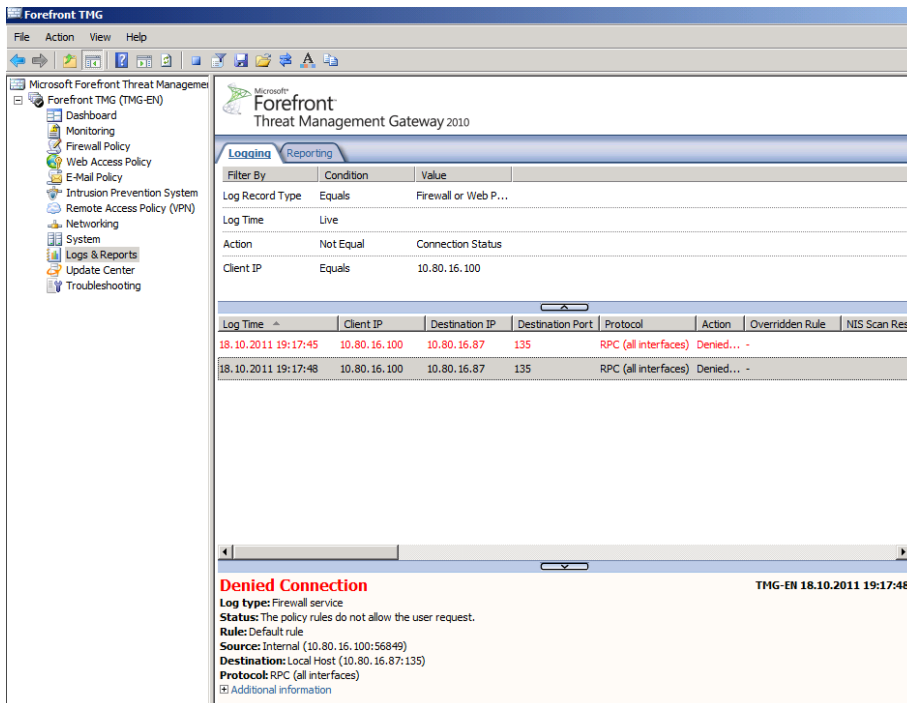


WMI Abfragen zu Forefront TMG erlauben

Testen zum Beispiel mit dem Paessler WMI Tester



RPC Anfragen werden verweigert, der WMI Tester kann nicht auf den Forefront TMG Server zugreifen, da die RPC Zugriffe verweigert werden



Erstellen einer Firewallregel welche RPC vom WMI Tester zum Forefront TMG Server erlaubt

All Firewall Policy								
Search... Examples								
Order	Name	Action	Protocols	From / Listener	To	Condition	Description	Policy
1	ALLOW-DC-WMI	Allow	RPC (all interfaces)	W2k8r2-en	Local Host	All Users		Array

Danach sieht es m TMG Logging besser aus, aber ...

Microsoft
Forefront
Threat Management Gateway 2010

Enterprise

Logging Reporting

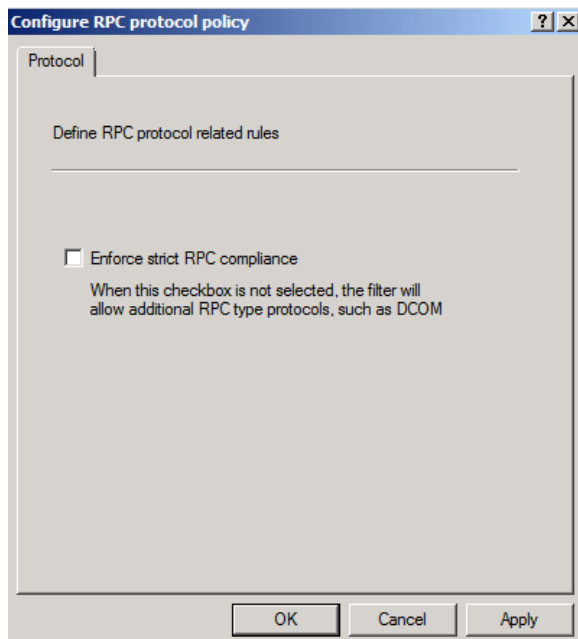
Filter By	Condition	Value
Log Record Type	Equals	Firewall or Web P...
Log Time	Live	
Action	Not Equal	Connection Status
Client IP	Equals	10.80.16.100

Log Time	Client IP	Destination IP	Destination Port	Protocol	Action	Overridden Rule	NIS Scan Result	NIS Signature	NIS Applicati
18.10.2011 19:20:42	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-			
18.10.2011 19:20:42	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Closed...	-			
18.10.2011 19:20:42	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-			
18.10.2011 19:20:42	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-			
18.10.2011 19:20:42	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Closed...	-			
18.10.2011 19:20:57	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Closed...	-			

Closed Connection TMG-EN 18.10.2011 19:20:57

Log type: Firewall service
 Status: Closed Connection
 Rule: ALLOW-DC-WMI
 Source: Internal (10.80.16.100:56854)
 Destination: Local Host (10.80.16.87:135)
 Protocol: RPC (all interfaces)
 Additional information

... weiterhin keine WMI Abfrageergebnisse im WMI Tester ☹. Also der Klassiker:
Enforce Strict RPC Compliance deaktivieren ...



Aber immer noch nicht viel besser. Jetzt sieht man im Log aber eine verweigerte Verbindung auf Port 10002 TCP und der Port scheint sich trotz RPC Dynamic zum Glueck nicht zu veraendern 😊

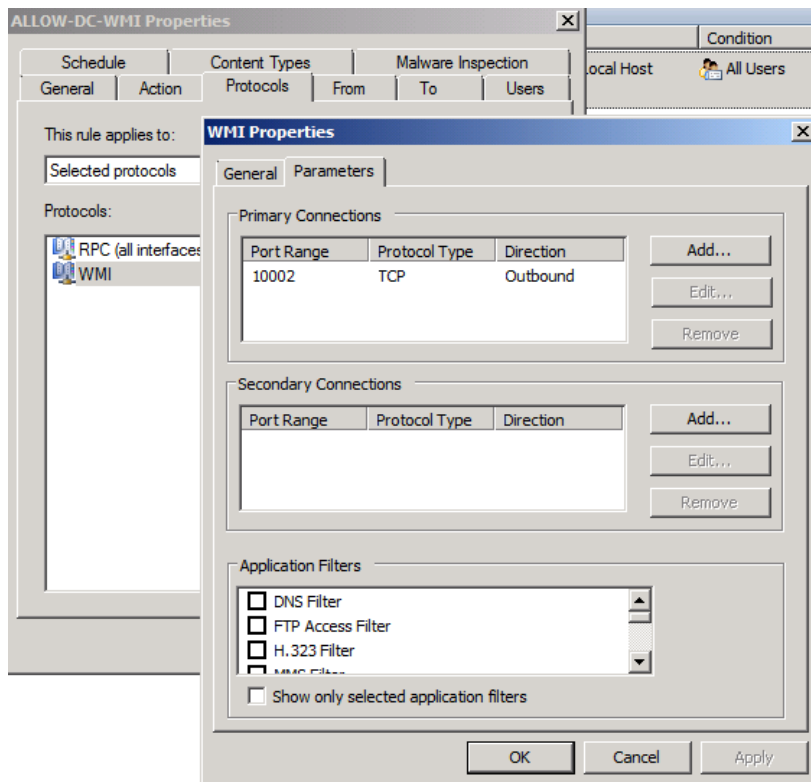
Microsoft Forefront Threat Management Gateway 2010 Enterprise

Logging Reporting

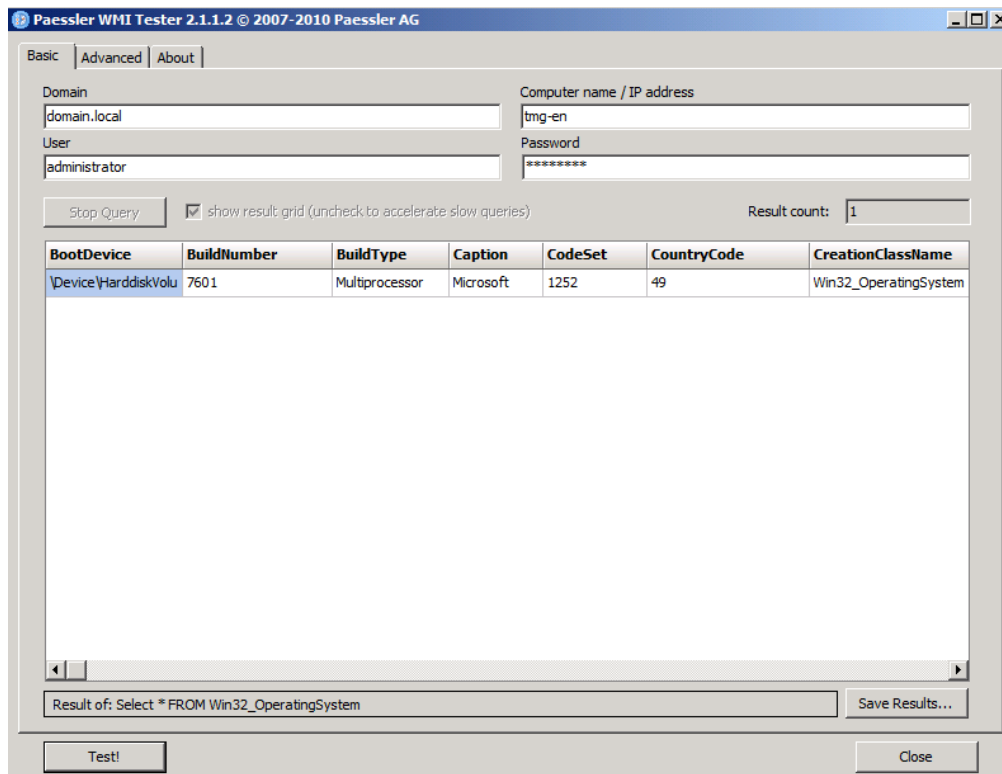
Filter By	Condition	Value
Log Record Type	Equals	Firewall or Web P...
Log Time	Live	
Action	Not Equal	Connection Status
Client IP	Equals	10.80.16.100

Log Time	Client IP	Destination IP	Destination Port	Protocol	Action	Overridden Rule	NIS Scan Result	NIS
18.10.2011 19:30:08	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-		
18.10.2011 19:30:08	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Closed ...	-		
18.10.2011 19:30:08	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-		
18.10.2011 19:30:08	10.80.16.100	10.80.16.87	135	RPC (all interfaces)	Initiate...	-		
18.10.2011 19:30:08	10.80.16.100	10.80.16.87	10002	Unidentified IP Traffic (TCP:10002)	Denied...	-		
18.10.2011 19:30:10	10.80.16.100	10.80.16.87	10002	Unidentified IP Traffic (TCP:10002)	Denied...	-		

Also die Firewallregel um ein neues benutzerdefiniertes Protokoll mit Port 10002 TCP erweitert ...



Danach funktioniert es!



Ob diese Firewallregel fuer jeden WMI Client ausreicht bleibt zu testen. Ich habe das ganze noch mit einem WMI Explorer getestet und damit hat es auch funktioniert.