Threat Management Gateway (TMG) System policy rules

https://technet.microsoft.com/en-us/library/cc441740.aspx

Updated: February 1, 2011

Applies To: Forefront Threat Management Gateway (TMG)

Forefront TMG system policy rules are a set of predefined access rules that control access between the Local Host network (the Forefront TMG server) and other networks. Some system policy rules are enabled by default to allow traffic that is necessary for managing the Forefront TMG environment. For more information, see About system policy. The following table lists the default system policy rules.

List order	Name	System policy group	Protocols	Source	Destination	Details
1	Allow access to directory services for authentication purposes	Authentication Services	LDAP LDAP (UDP) LDAP GC (Global Catalog) LDAPS LDAPS GC (Global Catalog)	Local Host	Internal	If Forefront TMG is not a domain member, this rule can be disabled.
2	Allow remote management from selected computers using MMC	Remote Management	Microsoft Firewall Control NetBIOS datagram NetBIOS Name Service NetBIOS Session RPC (all interfaces)	Array Servers Enterprise Remote Management Computers Remote Management Computers	Local Host	If you do not need a remote MMC connection to the Forefront TMG computer, this rule can be disabled. When this rule is enabled, RPC traffic is allowed to the Local Host network. However, by default, DCOM traffic is blocked by the RPC filter. Remote management computers must be added to the predefined Remote Management Computers computer set.
3	Allow remote management from selected computers using Terminal Server	Remote Management	RDP (Terminal Services)	Enterprise Remote Management Computers Remote	Local Host	If you do not need remote desktop management of the Forefront TMG computer, disable this rule. Remote

List order	Name	System policy group	Protocols	Source	Destination	Details
				Management Computers		management computers must be added to the predefined Remote Management Computers computer set.
4	Allow remote management from selected computers using a Web application	Remote Management	Forefront TMG Web Management	Enterprise Remote Management Computers Remote Management Computers	Local Host	If you do not need remote management from a Web application, disable this rule. Remote management computers must be added to the predefined Remote Management Computers computer set.
5	Allow remote logging to trusted servers using NetBIOS (disabled by default)	Remote Logging	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Local Host	Internal	Enable this rule if you are logging on to a remote SQL server.
6	Allow RADIUS authentication from Forefront TMG to trusted RADIUS servers	Authentication Services	RADIUS RADIUS Accounting	Local Host	Internal	If you are not using RADIUS authentication, disable this rule. If you are, limit the destination to the IP address of the RADIUS server.
7	Allow Kerberos authentication from Forefront TMG to trusted servers	Authentication Services	Kerberos-Sec (TCP) Kerberos-Sec (UDP)	Local Host	Internal	If you are not authenticating clients, disable this rule.
8	Allow DNS from Forefront TMG to selected servers	Network Services	DNS	Local Host	All Networks (and Local Host)	This rule must be enabled for Forefront TMG to perform DNS queries.
9	Allow DHCP requests from Forefront TMG to all networks	Network Services	DHCP (request)	Local Host	Anywhere	If the Forefront TMG computer does not need to be a DHCP client, disable this rule.
10	Allow DHCP replies from DHCP servers to Forefront TMG	Network Services	DHCP (reply)	Internal	Local Host	If the Forefront TMG computer does not need to be a DHCP client, disable

List order	Name	System policy group	Protocols	Source	Destination	Details
						this rule. If the DHCP server is not in the Internal network, change the Source property.
11	Allow ICMP (PING) requests from selected computers to Forefront TMG	Diagnostic Services	PING	Enterprise Remote Management Computers Remote Management Computers	Local Host	Any computer that must ping the Forefront TMG computer must be included in the Remote Management Computers computer set.
12	Allow ICMP requests from Forefront TMG to selected servers	Diagnostic Services	ICMP Information Request ICMP Timestamp PING	Local Host	All Networks (and Local Host)	This rule must be enabled to allow Forefront TMG to perform network management tasks.
13	Allow VPN client traffic to Forefront TMG (disabled by default)	This system policy rule is not modified through the system policy editor.	PPTP	External	Local Host	This rule is enabled automatically by Forefront TMG when you enable VPN traffic in Forefront TMG Management.
14	Allow VPN site-to-site traffic to Forefront TMG (disabled by default).	This system policy rule is not modified through the system policy editor.	None	External IPSec Remote Gateways	Local Host	This rule is enabled automatically by Forefront TMG when you create a site-to-site network in Forefront TMG Management.
15	Allow VPN site to site traffic from Forefront TMG (disabled by default)	This system policy rule is not modified through the system policy editor.	None	Local Host	External IPSec Remote Gateways	This rule is enabled automatically by Forefront TMG when you create a site-to-site network in Forefront TMG Management.
16	Allow Microsoft CIFS from Forefront TMG to trusted servers	Authentication Services	Microsoft CIFS (TCP) Microsoft CIFS (UDP)	Local Host	Internal	If you do not need to access file shares from the Forefront TMG computer, disable this rule.
17	Allow remote SQL logging from Forefront TMG to selected servers (disabled by default)	Remote Logging	Microsoft SQL (TCP) Microsoft SQL (UDP)	Local Host	Internal	Enable this rule if you are logging to a remote SQL server
18	Allow all HTTP traffic from	Authentication Services	HTTP	Local Host	All Networks (and Local Host)	Enable this rule to allow the Forefront

List order	Name	System policy group	Protocols	Source	Destination	Details
	Forefront TMG to all networks (for CRL downloads) (disabled by default)					TMG to access certificate revocation lists. This is required if you are bridging the SSL connection on the Forefront TMG computer. Configure the destination to specify only the network from which the CRL is downloaded.
19	Allow HTTP/HTTPS requests from Forefront TMG to selected servers for connectivity verifiers (disabled by default)	Diagnostic Services	HTTP HTTPS	Local Host	All Networks (and Local Host)	This rule is enabled automatically when you create a connectivity verifier.
20	Allow remote performance monitoring of Forefront TMG from trusted servers (disabled by default)	Remote Monitoring	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Enterprise Remote Management Computers Remote Management Computers	Local Host	Enable this rule to allow remote performing monitoring of Forefront TMG.
21	Allow NetBIOS from Forefront TMG to trusted servers	Diagnostic Services	NetBIOS datagram NetBIOS Name Service NetBIOS Sessions	Local Host	Internal	If you do not plan to access file shares from the Forefront TMG computer, disable this rule.
22	Allow RPC from Forefront TMG to trusted servers	Authentication Services	RPC (all interfaces)	Local Host	Internal	If you do not need to connect from the Forefront TMG computer to other servers using the RPC protocol, disable this rule.
23	Allow HTTP/HTTPS from Forefront TMG to specified Microsoft error reporting sites	Diagnostic Services	HTTP HTTPS	Local Host	Microsoft Error Reporting Sites	This rule allows error reports to be sent to Microsoft.
24	Allow SecurID authentication from Forefront TMG to trusted	Authentication Services	SecurID	Local Host	Internal	If you are not using SecurID authentication, disable this rule. If

List order	Name	System policy group	Protocols	Source	Destination	Details
	servers (disabled by default)					you are, limit the destination to the IP address of the RADIUS server.
25	Allow remote monitoring from Forefront TMG to trusted servers, using Microsoft Operations Manager (MOM) agent (disabled by default)	Remote Monitoring	Microsoft Operations Manager Agent System Center Operation Manager Agent	Local Host	• Forefront Protection Manager Gateway • System Center Operations Manager Servers for Forefront Protection Manager	Enable this rule if you are using MOM to monitor the Forefront TMG computer.
26	Allow installation of System Center Operations Manager Agent	Remote Monitoring	System Center Operation Manager Agent Installation	Local Host	Protection Manager gateway	This rule is required to allow the installation of System Center Operations Manager Agent.
27	Allow HTTP/HTTPS requests from Forefront TMG to specified sites	Various	HTTP HTTPS	Local Host	System Policy Allowed Sites URL Filtering Update Sites	This rule is required to allow the Forefront TMG computer to communicate with site in the System Policy Allowed Sites domain name set.
28	Allow HTTP/HTTPS requests from Forefront TMG to specified Microsoft Updates sites	Various	HTTP HTTPS	Local Host	Microsoft Update Sites	This rule is required to allow the Forefront TMG computer to communicate with Microsoft Updates sites listed in the Microsoft Update Domain Name Set.
29	Allow NTP from Forefront TMG to trusted NTP servers	Network Services	NTP (UDP)	Local Host	Internal	This rule allows Forefront TMG to contact NTP servers in the Internal network. Limit the destination to the IP address of the NTP server.
30	Allow SMTP from Forefront TMG to trusted servers	Remote Monitoring	SMTP	Local Host	Internal	If you do not intend to send SMTP alerts, disable this rule. Otherwise, limit the destination to the IP address of the SMTP server, instead of

List order	Name	System policy group	Protocols	Source	Destination	Details
						the Internal network.
31	Allow HTTP from Forefront TMG to selected computers for Content Download Jobs (disabled by default)	Various	HTTP	Local Host	All Networks (and Local Host)	This rule is automatically enabled when you create a Content Download Job in Forefront TMG Management.
32	Allow MS Firewall Control communication to selected computers	Remote Management	MS Firewall Control MS Firewall Storage	Local Host	Enterprise Remote Management Computers Remote Management Computers	If you are not using remote MMC, disable this rule.
33	Allow remote access to Configuration Storage server	Configuration Storage Servers	MS Firewall Control MS Firewall Storage	Local Host	All Networks (and Local Host) Enterprise Configuration Storage Servers	This rule is not relevant for Forefront TMG in the Essential Business Server scenario.
34	Allow access from trusted servers to the local Configuration Storage server	Configuration Storage Servers	Microsoft CIFS (TCP) Microsoft CIFS (UDP) MS Firewall Control MS Firewall Storage	Local Host Array Servers Enterprise Remote Management Computers Managed Forefront TMG Computers Remote Management Computers Replicate Configuration Storage Servers	Local Host	This rule is not relevant for Forefront TMG in the Essential Business Server scenario.
35	Allow replication between Configuration Storage servers	Configuration Storage Servers	MS Firewall Storage Replication RPC (all interfaces)	Local Host Replicate Configuration Storage Servers	Local Host Replicate Configuration Storage Servers	This rule is not relevant for Forefront TMG in the Essential Business Server scenario.
36	Allow intra-array communication	Intra-array Communication	Microsoft CIFS (TCP) Microsoft CIFS	Array Servers	Array Servers	This rule is not relevant for Forefront TMG in the Essential

List order	Name	System policy group	Protocols	Source	Destination	Details
			(UDP) Microsoft SQL (TCP) MS Firewall Control RPC (all interfaces)			Business Server scenario.
37	Allow IPv6 infrastructure traffic from local-host to IPv6 networks rule	Various	ICMPv6 Listener Done ICMPv6 Listener Query ICMPv6 Listener Report ICMPv6 Listener Report v2 ICMPv6 Multicast Router Advertisement ICMPv6 Multicast Router Solicitation ICMPv6 Multicast Router Termination ICMPv6 Neighbor Advertisement ICMPv6 Neighbor Solicitation ICMPv6 Router Advertisement ICMPv6 Router Solicitation	Local Host	Internal	This rule allows IPv6 infrastructure traffic from local-host to IPv6 networks.
38	Allow IPv6 infrastructure traffic from IPv6 networks to local-host rule	Various	ICMPv6 Listener Done ICMPv6 Listener Query ICMPv6 Listener Report	Internal	Loacl Host	This rule allows IPv6 infrastructure traffic from IPv6 networks to local-host rule.

List order	Name	System policy group	Protocols	Source	Destination	Details
			ICMPv6 Listener Report v2 ICMPv6 Multicast Router Advertisement ICMPv6 Multicast Router Solicitation ICMPv6 Multicast Router Termination ICMPv6 Neighbor Advertisement ICMPv6 Neighbor Solicitation ICMPv6 Router Advertisement ICMPv6 Router Solicitation Link-local multicast name resolution			
39	Blocks access from Protection Manager Blocked Access Computers to the External network	Network Services	All Outbound Traffic	Protection Manager Blocked Access Computers Protection Manager Exempt Computers	All Networks (and Local Host)	This rule blocks access from the computers in the Protection Manager Blocked Access Computers computer set to the External network.
40	Restricts access from Protection Manager Limited Access Computers to the External network	Network Services	All Outbound Traffic	Protection Manager Blocked Access Computers Protection Manager Exempt Computers	All Networks (and Local Host) Approved URLs for Protection Manager policies	This rule allows access from the computers in the Protection Manager Limited Access Computers to URLs approved for Protection Manager policies.
41	Allow access between local host and the Protection	Network Services	Forefront codename Stirling WS	Internal Local Host	Local Host Forefront codename Stirling gateway	This rule allows traffic between the Forefront TMG server and the

List order	Name	System policy group	Protocols	Source	Destination	Details
	Manager gateway					Protection Manager gateway.
42	Allow Notifications to Forefront TMG Client	Various	Allow Notifications to Forefront TMG Client	Local Host	Internal Quarantined VPN Clients VPN Clients	This rule allows notifications from Forefront TMG to the Forefront TMG Client software on client computers.
43	Allow access from local host to Forefront codename Stirling core server	Network Services	WCF	Local Host	Forefront codename Stirling core servers	This rule allows access from the Forefront TMG server to the Forefront codename Stirling core server.
44	Allow SMTP traffic to the local host for mail protection and filtering	Various	SMTP	All Networks (and Local Host)	Local Host	This rule allows SMTP traffic from the internet to the local host for advanced Antispam and Content filtering and Malware protection.
45	Allow SMTP traffic to the internet for mail protection and filtering	Various	SMTP	Local Host	All Networks (and Local Host)	This rule allows SMTP traffic to from the local host to the internet for advanced Antispam and Content filtering and Malware protection.
46	SSTP Publishing	Network Services	None	None	Local Host	SSTP publishing rule for allowing VPN roaming clients connections using SSTP protocol.
47	Allow LDAP/LDAPS traffic to the local host for the Exchange Server EdgeSync synchronization process	Network Services	LDAP(EdgeSync) LDAPS(EdgeSync)	Internal	Local Host	This rule allows LDAP/LDAPS traffic to the local host for the Exchange Server EdgeSync synchronization process.
48	Direct Access mode: Allow restricted set of protocols over IPv6 to local-host rule	Various	DHCPv6 ICMPv6 Echo ICMPv6 Listener Done ICMPv6 Listener Query ICMPv6 Listener	Anywhere (IPv6)	Local Host	This rule allows restricted set of protocols over IPv6 in DirectAccess mode to local-host rule.

List order	Name	System policy group	Protocols	Source	Destination	Details
			Report ICMPv6 Listener Report v2 ICMPv6 Multicast Router Advertisement ICMPv6 Multicast Router Solicitation ICMPv6 Multicast Router Termination ICMPv6 Neighbor Advertisement ICMPv6 Neighbor Solicitation ICMPv6 Router Advertisement ICMPv6 Router Solicitation IKE Server Link-local multicast name resolution			
49	Direct Access mode: Allow IPv6 transition technologies traffic to local-host rule	Various	HTTPS IPv6 Over IPv4 Tunnel Teredo Server	All Networks (and Local Host)	Local Host	This rule allows IPv6 transition technologies traffic in DirectAccess mode to local-host rule.
50	Direct Access mode: Allow IPv6 traffic from local-host rule	Various	All Outbound Traffic	Local Host	Anywhere (IPv6)	This rule allows IPv6 traffic in DirectAccess mode from local-host rule.