

# SecureFirst

CONFIGURING NETWORK MONITOR POLICIES TO MONITOR A NETWORK PATH VIABILITY

KNOWLEDGE DATABASE



## CONFIGURING NETWORK MONITOR POLICIES TO MONITOR A NETWORK PATH VIABILITY

### **DESCRIPTION:**

Configuring Network Monitor Policies to monitor a network path viability

### **RESOLUTION:**

The Network | Network Monitor page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the Network Monitor page, and are also provided to affected client components and logged in the system log.

Each custom NM (Network Monitor) policy defines a destination Address Object to be probed. This **Address Object** may be a Host, Group, Range, or FQDN. When the destination **Address Object** is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

### Network Monitor

ietwork Monitor Pol	icies											Items		to 2 (of 2)	(1 4	
riew Style: 🏾 All Poli	cies C Custor	m Policies														
Add.	Delote											Clear SI	alistics		Delete /	A.E
E # Name	Probe Target	Gateway	Local IP In	terface Probe	е Туре	Interval	Port	Response Timeout	Falure Threshold	Success Threshold	All Must Res	pond 9	atus	Comment	Confi	gure
C 0 TestProbe	DNS			Ping	1 8	5		1	3	3	No	9		ø	Ø	×
🗖 1 License Server	License Server			TCP	1	5	443	1	3	3	Yes			ø	Ø	×
Add	Delete										0	Clear St	atistics		Delete A	All .

# The **Status** column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.

• Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.

The following information is displayed in the probe status:

C	nreshold All Must	Clear St.	Resolved I Probes Se Responses Probe Tarr	% Successful Probe Targets: 1 ht: 35035 5 Received: 22486 gets: pwn / 0 Unknown	5
Duccess n	incontoita. Minimase	Respond Se	2	1000	
3	No	0		Ø	
3	Yes	0	10	Ø	
		Clear Sta	tistics	Delete All	]

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.

• A list of resolved probe targets, and their status.

Adding a Network Monitor Policy To add a network monitor policy on the SonicWall security appliance, perform these steps:

Step 1From the Network | NetworkMonitor page, click the Add button. The AddNetwork Monitor Policy window is displayed.





etwork Monitor F	Policy Settings			Name:	License Server	1				
lame:	License Server			Zone Assignment: Type:	WAN FODN					
robe Target:	License Server	-	-							
iext Hop Gateway:	Select an address object			FQDN Hostname:		er.sonicwall.com				
ocal IP Address:	Select an address object V			Manually set DNS	(120~86400s)					
Outbound Interface:	X0			Ready						
	Probe type	Ping (ICMP	)			OK		Cancel		
	Port			here -		Clear Sta	tistics	De		
	Probe hosts every	5 st	econds							
	Reply time out	1 st	econds							
	Probe state is set to DOWN after	3 m	issed interva	5						
	Probe state is set to UP after	3 s	uccessful inte	rvals						
	All Hosts Must Respond									
	RST Response Counts As M	55								
Comment:										

**Step 2** Enter the following information to define the network monitor policy:

• Name - Enter a description of the Network Monitor policy.

• **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting Create New Address Object.

• **Probe Type** - Select the appropriate type of probe for the network monitor policy:

– **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified **Response Timeout** time limit for the ping to be counted as successful.

- **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via thesame interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

- **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the **Outbound Interface** pull down menu to send a Ping to the targets. If a **Next Hop Gateway** is not specified, the probe assumes that the targets are directly connected to the **Outbound Interface**'s network.

- TCP - Explicit Route - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pull down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

– Next Hop Gateway - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.

• **Outbound Interface** - Manually specifies which interface is used to send the probe. This option must be configured for **Explicit Route** policies. For **non-Explicit Route** policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.

• **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes.



SONICWALL<sup>®</sup> Knowledge Database

**Step 3** Optionally, you can adjust the following thresholds for the probes:

• **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field.

• **Reply time out** - The number of seconds the **Network Monitor** waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The **Reply time out** cannot exceed the **Probe hosts every** field.

• **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN.

• **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP.

• All Hosts Must Respond - Selecting this checkbox specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP.

Step 4 Optionally, you can enter a descriptive comment about the policy in the Comment field.Step 5 Click Add to submit the Network Monitor policy.

### Example 1:

Using Network Monitor Probes in Policy Based Routing

**Network Monitor policy** can be used, when configuring a static route, as a condition to dynamically enable or disable the static route. When a **Network Monitor policy** is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

	Any	×
Destination:	Remote Network	~
Service:	Any	~
Gateway:	Router on DMZ	~
Interface:	X0	~
Metric:	1	
Comment:		
	Disable route when the interface is disconnected	
	Allow VPN path to take precedence	
WXA Group:	None	~
Probe:	TestProbe	~
	Disable route when probe succeeds	

General

In the example above, a static route has been created to route traffic to a remote network which is reachable through a router on the DMZ. Under the **Probe** a **Network Monitor Policy** has been selected which pings a host on the remote network. Failure of the ping will result in disabling this route. Typical configurations will not check the **Disable route when probe succeeds** checkbox, because typically administrators will want to disable a route when a probe to the route's destination fails. This option is provided to give administrators added flexibility for defining routes and probes.

The **Probe default state is UP** option is to have the route consider the probe to be successful (i.e. in the "UP" state) when the attached Network Monitor policy is in the "UNKNOWN" state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from "IDLE" to



Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290/+57 318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01



"ACTIVE," because this transition sets all Network Monitor policy states to "UNKNOWN."

### Example 2:

Using Network Monitor policies in Route Policies to dynamically failover between VPN and MPLS connection

This following article illustrates a scenario wherein two sites with SonicWall UTM devices are connected to each other over a direct connection or an MPLS connection. A site to site VPN connection is defined concurrently between the two sites. The primary connection between the two sites is the direct or the MPLS connection and when it fails, traffic would automatically be routed through a site to site VPN (policy based).

For detailed instructions please refer to <u>KB ID</u> 8445

### Logs messages:

Here is a sample log message when the Network Monitoring probe goes Down

Alert	Network Monitor	Network Monitor: Policy test status is DOWN
Alert	Network Monitor	Network Monitor: Host 192, 168, 168, 65 (Policy:test) is offline

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

The **Investigate** in the top navigation menu Under **Network Probes** page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the **Network Probes** page, and are also provided to affected client components and logged in the system log.

Each custom NM (Network Probe) policy defines a

destination Address Object to be probed. This **Address Object** may be a Host, Group, Range, or FQDN. When the destination **Address Object** is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

1. Click **Investigate** in the top navigation menu.

2. Click on **Network Probes**.

3. Click on **configure** button to configure network probes policy.

														Mod	le: Confi	guration
.ogs																
Event Logs												Iter	ns 1	to 2 (	of 2) 📻	4.4
Connection Logs	View S	to day	• All Po		00	tom Pol		Man	P Version		IPv4 On		Pv6 Onl		IPv4 and	
ppflow Logs VAN Acceleration Logs	view 5	cyte:	C All PC	licies	Cu	stom Poi	ICIES	view 1	P version	•	IPv4 Un	γ U Ι	Pvo Uni	y 0	IPV4 and	I IPV0
Anti-Spam Junkbox	1	ADD									CLE	AR STAT	ISTICS		DELET	e all.
teports		Name	Prob	Gate	Loca	Inte	Prob	Inte I	Port Resp	Failu	Succ	All M	RST	Status	Com	Con.
ppflow Reports		TestP	8.8.8.8				Ping	5	1	3	3	No	N/A		ø	
og Reports RF Analysis	2	Licen	License Server				Ping	5	1	3	3	Yes	N/A		ø	Ø
AN Acceleration Reports	-	ADD	1	DELETE							CLE	NR STAT	ISTICS		DELET	E ALL
CP Acceleration Reports																
/FS Acceleration Reports																
VXA Web Cache Reports																
ools																
acket Monitor																

The **Status** column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.

The following information is displayed in the probe status:



'ersion:	Probe Resol Probe Respo	ved Prob es Sent: 2 onses Re e Targets	Successfu e Targets: 233 ceived: 233	1 Pv6 Only I		o 2 (of 2) IN THE PART O IPv4 and IPv6							
Resp	Targe	et 8.8.8.8	UPAILM	RST	atus	Com	Con						
1	3	3	No	N/A	0	Ø	Ø						
1	3	3	Yes	N/A	۲	Ø	Ø						

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

### Adding a Network Monitor Policy To add a network monitor policy on the SonicWall security appliance, perform these steps:

1. Click **Investigate** in the top navigation menu.

2. Click on Network Probes.

3. Click on configure button to configure network probes policy.

The Add Network Monitor Policy window is displayed.





**Step 2** Enter the following information to define the network monitor policy:

• Name - Enter a description of the Network Monitor policy.

• **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting Create New Address Object.

• **Probe Type** - Select the appropriate type of probe for the network monitor policy:

**Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified **Response Timeout** time limit for the ping to be counted as successful.

- TCP - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via thesame interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

- **Ping (ICMP)** - **Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the **Outbound Interface** pull down menu to send a Ping to the targets. If a **Next Hop Gateway** is not specified, the probe assumes that the targets are directly connected to the **Outbound Interface**'s network.

- TCP - Explicit Route - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pull down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly





connected to the **Outbound Interface**'s network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

- Next Hop Gateway - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.

• **Outbound Interface** - Manually specifies which interface is used to send the probe. This option must be configured for **Explicit Route** policies. For **non-Explicit Route** policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.

• **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes.

**Step 3** Optionally, you can adjust the following thresholds for the probes:

• **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field.

• **Reply time out** - The number of seconds the **Network Monitor** waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The **Reply time out** cannot exceed the **Probe hosts every** field.

• **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN.

• **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP.

• All Hosts Must Respond - Selecting this checkbox specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked,

the **Policy State** is set to UP when any of the **Host States** are UP.

Step 4 Optionally, you can enter a descriptive comment about the policy in the Comment field.Step 5 Click Add to submit the Network Monitor policy.

### **Example 1:**

Using Network Monitor Probes in Policy Based Routing

**Network Monitor policy** can be used, when configuring a static route, as a condition to dynamically enable or disable the static route. When a **Network Monitor policy** is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

Genera	al	
Route Poli	cy Settings	
Source:	Any	~
Destination:	Remote Network	~
Service:	Any	~
Sateway:	Router on DMZ	~
Interface:	X0	×
Metric:	1	
Comment:		
	Disable route when the interface is disconnect	ed
	Allow VPN path to take precedence	
WXA Group:	None	~
robe:	TestProbe	~
	Disable route when probe succeeds	
	Probe default state is UP	

In the example above, a static route has been created to route traffic to a remote network which is reachable through a router on the DMZ. Under the **Probe a Network Monitor Policy** has been





selected which pings a host on the remote network. Failure of the ping will result in disabling this route. Typical configurations will not check the **Disable route when probe succeeds** checkbox, because typically administrators will want to disable a route when a probe to the route's destination fails. This option is provided to give administrators added flexibility for defining routes and probes.

The **Probe default state is UP** option is to have the route consider the probe to be successful (i.e. in the "UP" state) when the attached Network Monitor policy is in the "UNKNOWN" state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from "IDLE" to "ACTIVE," because this transition sets all Network Monitor policy states to "UNKNOWN."

**Example 2:** 

Using Network Monitor policies in Route Policies to dynamically failover between VPN and MPLS connection

This following article illustrates a scenario wherein two sites with SonicWall UTM devices are connected to each other over a direct connection or an MPLS connection. A site to site VPN connection is defined concurrently between the two sites. The primary connection between the two sites is the direct or the MPLS connection and when it fails, traffic would automatically be routed through a site to site VPN (policy based).

For detailed instructions please refer to <u>KB ID</u> <u>8445</u>

Logs messages:

Here is a sample log message when the Network Monitoring probe goes Down

1. Click **Investigate** in the top navigation menu.

2. Click on Event Logs

SONICWALL	Network Security Appl	lance	MONI		VESTIGATE	MAN	AGE	QUI	CK CC	NFIG	URATION
Logs	+ Filter View										
Connection Logs	Search			Show Las	t 30 minutes 💌	C	Q	8.	S	0	Go to Configu
Appflow Logs WAN Acceleration Logs	Local Time +	ID	Category	Priority	Message						
Anti-Spam Junkbox	01:44:45 Aug 29	1102	Network	Alert	Network Monitors	Policy L	icense 5	erver statu	is is DOV	WN .	
Proventer	01:44:45 Aug 29	706	Network	Alert	Network Monitor: I	Host 25	4.212.1	0.143 (Po	licyclice	nse Serv	rer) is offline



Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01