

WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- SD-WAN action enhancements
- SD-WAN reporting enhancements
- Link Monitor enhancements
- WebBlocker Warn action
- DNSWatch available in Bridge Mode
- IPv6 support for BOVPN and BOVPN virtual interfaces
- Support for multiple syslog servers
- Proxy support for TLS v1.3
- Enhanced FireCluster Diagnostics page



- Geolocation Deny message
- Exceptions/Blocked Sites List enhancements
- Synchronize feature key enhancements
- Proxy enhancements for DNSWatch
- FQDN limit increase
- MD5 in Gateway AV/IntelligentAV logs
- RADIUS and SecurID enhancements
- SSO Debug Tool enhancements
- Access Portal RDP enhancements



- Technology Integrations page updates
- Device configuration template updates
 - QoS
 - DNS/WINS
 - WebBlocker Warn action
- Edit 1-to-1 NAT in the Web UI



SD-WAN Enhancements



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

SD-WAN Enhancements

- As development continues on our SD-WAN solution, SD-WAN benefits now extend to more than just external WAN connections
- With these enhancements, you can now downsize or eliminate expensive MPLS connections
 - For example, an SD-WAN implementation with BOVPN virtual interfaces and metrics-based failover gives you encrypted tunnels over the public Internet plus reliability



SD-WAN Enhancements

- SD-WAN actions now support:
 - Multiple BOVPN virtual interfaces
 - Internal interfaces (Trusted, Optional, and Custom)
- With these enhancements, you can now:
 - Measure loss, latency, and jitter on internal interfaces and BOVPN virtual interfaces
 - Fail over based on loss, latency, and jitter for internal interfaces and BOVPN virtual interfaces
 - Use a policy and SD-WAN action to route traffic on any interface

- This includes internal interfaces configured for private network links

SD-WAN — BOVPN Virtual Interface Failover

 You can now configure BOVPN virtual interface failover in an SD-WAN action

	nacemen		
cription: BC	OVPN virtual interface to Data	icenter	
-WAN Inter elect the int ther than th	faces erfaces to include in this SD- e default gateway. To chang	WAN action. For useful loss, latency, and jitter metrics, we recommented to a target, edit the Link Monitor configuration.	nd that you specify targets
Include	Interface	Targets	Move Up
	BovpnVif.2	Ping (Virtual Peer IP)	
\square	BovpnVif.1	Ping (Virtual Peer IP)	Move Dow
	External-2	Ping (4.4.4.4)	
trics Setting elect measu ny selected	External gs	Ping (8.8.8.9) that determine when failover occurs to another SD-WAN interface. F	ailover occurs if the value
trics Setting ielect measu ny selected Loss Ra	External ps urements and specify values measurement is exceeded. te 5	Ping (8.8.8.9)	ailover occurs if the value
etrics Setting elect measury selected Loss Ra	External gs urements and specify values measurement is exceeded. te 5 - % 20 - ms	Ping (8.8.8.9)	ailover occurs if the value
trics Setting select measu ny selected Loss Ra Latency	External gs urements and specify values measurement is exceeded. te 5 • % 20 • ms 10 • ms	Ping (8.8.8.9)	ailover occurs if the value
etrics Setting iselect measury Selected Loss Rai Latency Jitter	External ps urements and specify values measurement is exceeded. te 5 • % 20 • ms 10 • ms if values for all selected mea	Ping (8.8.8.9) that determine when failover occurs to another SD-WAN interface. F asurements are exceeded.	ailover occurs if the value
trics Setting elect measury selected Loss Rai Latency Jitter Fail over	External gs urements and specify values measurement is exceeded. te 5 - % 20 - ms 10 - ms if values for all selected measurements the Einstein bandles for the selected	Ping (8.8.8.9) that determine when failover occurs to another SD-WAN interface. F asurements are exceeded.	ailover occurs if the value
trics Setting elect measury selected Loss Ra Latency Jitter Fail over ilback for Ad	External gs urements and specify values measurement is exceeded. te 5 + % 20 + ms 10 + ms if values for all selected measures tive Connections he Firebox handles failback f	Ping (8.8.8.9) that determine when failover occurs to another SD-WAN interface. F asurements are exceeded.	ailover occurs if the value

SD-WAN — **BOVPN** Virtual Interface Failover

- You can select to fail over based on loss, latency, or jitter measurements
 - If you do not select any measurements, failover occurs if the primary connection fails
- Requirements for BOVPN virtual interface failover:
 - In the BOVPN virtual interface settings for both interfaces, you must configure a virtual peer IP address
 - The virtual peer IP address must be an IP address and not a netmask
 - You must add both interfaces to Link Monitor. For BOVPN virtual interfaces, the link monitor target is the virtual peer IP address and cannot be changed

- You can now include internal interfaces in an SD-WAN configuration
 - This includes Trusted, Optional, and Custom interfaces
- If you have a private network connection such as a private line, leased line, or MPLS configured on an internal interface, you can configure SD-WAN failover to another connection

- Example topology
 - An MPLS connection is the primary connection for traffic to a remote data center
 - The MPLS connection uses an internal interface on the Firebox
 - The BOVPN virtual interface is configured as a failover interface





WatchGuard Training

Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- Example configuration at the local site (the branch office)
 - In the Link Monitor settings, add the BOVPN virtual interface and the internal interface used for the MPLS connection

K Network Configuration											×			
Interfaces Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPoE				
Link Monitor Configuration		S	ettings: Specify th action with routing tab Next h Select the replaced.	e next hope for {0} this interface can le will be used to for op:	. This is prefibe routed to orward probi	erred so that the the next hop. If ing traffic and tr 0}. If you add cu target is used.	probing traf the next hop affic using SI stom targets	ffic and traffic is not specifi D-WAN action , the default g	using an Si ed, the norm with this in ateway targ	D-WAN nal Iterface. get is				
				Туре	1	Target	Measure L	oss, Latency, ace to Monit	a Ad Ed	id			;	×
			Require	e a successful prot	pe to all targe	ets to	Name			Туре		Zone]	7
			Probe	Interval: 5	Seconds	s Extern	al-2	F	All Physical		~	All External	~	
Add			Deactivat Reactivat	te After: 3 te After: 3	Consecut Consecut	utive Bovpr utive Truste	Vif.1 d	F	BOVPN Virtu Physical Physical	ual Interfa	ace	Trusted Trusted		
Add						Extern	al-1	₹	hysical			External		
												<u>O</u> K	C <u>a</u> ncel	٦

- For the MPLS interface, specify the IP address of the next hop
 - In our example, the next hop is the local side of the local MPLS router

	Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPo
ink Monitor	Configuration										
Monitored	Interfaces:		Set	ttings:							
BovpnV MPLS	if.1			Specify the SD-WAN ac normal routi interface. Next hop Select the ta	next hope for MPI tion with this interf ng table will be use b: 10.0.2 argets to verify the Otherwise the de	LS. This is priface can be r ed to forward 2.2 status of MI	referred so that it routed to the nex d probing traffic PLS. If you add	the probing tr tt hop. If the i and traffic us custom targe	affic and traff next hop is not sing SD-WAN a ets, the default	ic using an t specified, t action with gateway ta	the this arget
				Туре	Tar	get	Measure Lo	ss, Latency,	and Jitter	Add	
				Ping	Next Hop		0			Edit	
										Delete	э
				Require Use these	a successful prob settings for MPLS	e to all target:	s to define the ir	iterface as a	ctive.		
				Probe In Deactivate Reactivate	terval: 5 After: 3 After: 3	Consecut Consecut	tive Failures tive Successes				

 The Link Monitor target for the BOVPN virtual interface is the IP address of the remote VPN peer

k Monitor	Configuration	Dingo	. 2	Loopback		millionento	by manife birto			00 11/1	
lonitored	Interfaces:		Se	ttings:							
BovpnV	if.1			Currently, for VPN	VIF, we on	ly support or	ne type of probi	ng target, by	default, I.E. pir	ng to peer	r virtual IP
MPLS				Туре		Т	arget	Measure L	oss, Latency,	a /	\dd
				Ping		Virtual Peer I	P	\odot		E	Edit
										C)elete
				Require a suc	cessful prob	e to all targe	ts to define the	interface as	active.		
				Use these setting	gs for Bovp	nVif.1:					
				Probe Interval	: 5	Seconds					
				Deactivate After	3	 Consecu 	tive Failures				
				Deactivate After	- 2	 Consecu 	tive Successes				
				Reactivate Atter	·[•					
∆dd	Delete										
	20.010										
Add	Delete										

 Next, add an SD-WAN action that includes the MPLS interface and the BOVPN virtual interface, and specify metric

	(accritic)		
cription:			
D-WAN Interf	aces		
other than the	erraces to include in this SD-v e default gateway. To change	a target, edit the Link Monitor configuration	commend that you specify targets
Include	Interface		Movello
	BovpnVif.1	Ping (Virtual Peer IP)	move op
	MPLS	Ping (Next Hop)	Move Down
	External	Ping (4.2.2.1)	
	External	Ding (9.9.9.9)	
		Fing (0.0.0)	
etrics Setting	s	hat determine when failwar occurs to another SD WAN inte	rface. Failever occurs if the value t
etrics Setting Select measu any selected ☑ Loss Rat	s rements and specify values th measurement is exceeded. e 5 + %	hat determine when failover occurs to another SD-WAN inte	rface. Failover occurs if the value f
etrics Setting Select measu any selected I Loss Rat Latency	s rements and specify values the measurement is exceeded. e 5 % 20 ms	hat determine when failover occurs to another SD-WAN inte	rface. Failover occurs if the value f
etrics Setting Select measu any selected U Loss Rat Latency Jitter	s rements and specify values ti measurement is exceeded. e 5 + % 20 + ms 10 + ms	hat determine when failover occurs to another SD-WAN inte	rface. Failover occurs if the value f
etrics Setting Select measu any selected ✓ Loss Rat ✓ Latency ✓ Jitter ◯ Fail over	s rements and specify values th measurement is exceeded. e 5 • % 20 • ms 10 • ms if values for all selected meas	hat determine when failover occurs to another SD-WAN inte	rface. Failover occurs if the value f
etrics Setting Select measu any selected Loss Rat Latency Jitter Fail over	s rements and specify values th measurement is exceeded. e 5 - % 20 - ms 10 - ms if values for all selected meas	hat determine when failover occurs to another SD-WAN inte	rface. Failover occurs if the value f
etrics Setting Select measu any selected U Loss Rat U Latency Jitter Fail over Select how th	s rements and specify values ti measurement is exceeded. e 5 % 20 ms 10 ms if values for all selected meas tive Connections re Firebox handles failback fo	hat determine when failover occurs to another SD-WAN inte surements are exceeded.	rface. Failover occurs if the value f

WatchGuard Training

settings

- Finally, add a policy that specifies the SD-WAN action
 - In our example, traffic that matches this policy is sent over the MPLS connection to the local network at the Datacenter
- If MPLS performance does not meet your requirements, or the link fails, traffic fails over to the BOVPN VIF

e: Sl	IP-ALG							🗹 Ena
icy P	Properties	Advanced						
ALG	connection	s are						
lowed	I	~	Send TC	PRST				· · · · · · · · · · · · · · · · · · ·
- 10.	.0.1.0/24							
					٨dd	Edit	F	Remove
					Auu			tomovo.
					Add			tomore
o 	.0.50.0/24				Add			
o 물 10.	.0.50.0/24				Add			
ठ ≱ 10.	.0.50.0/24				Add	Edit		Remove
o 4 4 4 10.	.0.50.0/24				Add	Edit	ļ	Remove
o 10. Roi	.0.50.0/24 ute outbour	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 c	For higher	Remove
0 ♣ 10. ✓ Roi SD-V	.0.50.0/24 ute outbour	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 c	pr higher	Remove)
₀ 불급 10. ☑ Roi SD-V	.0.50.0/24 ute outbour	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 o	Pr higher	Remove)
이	.0.50.0/24 ute outbour	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 d	pr higher	Remove)
o ≟ 10. ∑ Roi SD-V	.0.50.0/24 ute outbour	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 d	pr higher	Remove)
"₀ "∰ 10. "∑ Rou SD-V	.0.50.0/24 ute outbour WAN Action	nd traffic usin	g SD-WA	N Based Rou	Add	Edit are OS v12.3 d	pr higher	Remove)
'o ♣ ₽ 10.	.0.50.0/24 ute outbour WAN Action	nd traffic usin	g SD-WA	N Based Rou	Add Firew	Edit are OS v12.3 o	pr higher	Remove)
'o '호 10. SD-V] Enab	.0.50.0/24 ute outbour WAN Action Die Applicat	nd traffic usin	g SD-WA	N Based Rou	Add ting Fireway Fireway	Edit are OS v12.3 d	pr higher	Remove
:o	.0.50.0/24 ute outbour WAN Action Die Applicat Die Geoloca	nd traffic usin Datacenter ion Control: tion his policy	g SD-WA	N Based Rou	Add ting Fireway Fireway	Edit are OS v12.3 d	pr higher	Remove)
io i 10. i 10.	.0.50.0/24 ute outbour WAN Action Die Applicat Die Geoloca Die IPS for ti	nd traffic usin Datacenter ion Control: tion his policy tth and time of	g SD-WA	N Based Rou	Add ting Firewa Firewa 10 and higher)	Edit are OS v12.3 o	pr higher	Remove)

- Static routes and SD-WAN
 - Different factors determine whether static routes are recommended or required
 - Sites that initiate traffic If both sites have Fireboxes configured with SD-WAN actions, you do not have to add a static route on a Firebox that initiates traffic in most cases
 - Sites that receive traffic We recommend that you add static routes on a Firebox at a site that receives traffic
 - You must add a static route if you did not specify a next hop IP address for an internal interface

- IP Spoof Attack protection and SD-WAN
 - If the global Drop Spoofing Attacks setting is enabled, the Firebox monitors inbound traffic on internal and external interfaces for IP spoof attacks
 - If the Firebox determines traffic is not an IP spoof attack, the Firebox sends reply traffic through the same interface as the inbound interface
 - For internal interfaces:
 - If the interface in the routing results does not match the inbound interface, the Firebox considers the inbound traffic to be an IP spoof attack
 - The Firebox drops the inbound traffic and does not send reply traffic
 - If you add static routes, make sure to configure route metrics correctly

SD-WAN

- Restrictions to interface type changes:
 - In most cases, you cannot change the interface type (zone) for an interface included in an SD-WAN action
 - If the interface type is internal (Trusted, Optional, or Custom) you can change the interface type to another internal type
 - For example, if a Trusted interface appears in an SD-WAN action, you can change the interface type to Optional or Custom

SD-WAN Configuration Conversion

- Important: Before you upgrade to Fireware v12.4 or higher, review the <u>Release-specific upgrade notes</u> in the WatchGuard Knowledge Base about a change that affects some inbound NAT policies with policy-based routing or an SD-WAN action
 - In Fireware v12.3.1 or lower, the Firebox ignored unnecessary policy-based routing or SD-WAN actions in inbound NAT policies
 - To support SD-WAN enhancements in v12.4, when you upgrade to Fireware v12.4 or higher:
 - For policies with a SNAT action to an <u>RFC1918</u> address, the Firebox automatically removes policy-based routing or SD-WAN actions to external interfaces unless the action specifies only a BOVPN virtual interface
 - RFC1918 includes the networks 192.168.0.0/16, 172.16.0.0/12, and 10.0.0/8

SD-WAN Configuration Conversion

- For policies with 1-to-1 NAT to an internal address:
 - The Firebox does not automatically remove policy-based routing or SD-WAN actions to external interfaces
 - We recommend that you manually remove any policy-based routing or SD-WAN action that is unnecessary



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- On the SD-WAN reporting page:
 - Internal interfaces (Trusted, Optional, and Custom) configured with Link Monitor targets now appear
 - BOVPN virtual interfaces configured with Link Monitor targets now appear
 - Interfaces are grouped by type instead of alphabetically
 - A maximum of 64 interfaces can appear in the Monitored Interfaces list
 - A maximum of 15 interfaces can appear simultaneously on each chart

 SD-WAN reporting page in the Web UI

Interfaces	20 MINUTES AGO 🔻	C
Bandwidth Detail SD-WAN		
All Monitored Interfaces v		
All Monitored Interfaces	er to see data for individual interfa	ace.
BovprVif.2(bvpn2)		
External(eth0) Trusted(eth1)		
External-2(eth3)		
Bow	pnVif.1 (bvpn1) Average	: N/A
75 %	pnVlf.2 (bvpn2)	
Exte	ernal (eth0) sted (eth1)	
50 %	ernal-2 (eth3)	
25 %		
0 %		
20 minutes ago	Now	
T shows i		
Latency		
0.200 ms		
Boy	pnVif.1 (bvpn1) Average	: N/A
0.150 ms	prVlf.2 (bvpn2)	
Trus	sted (eth1)	
0.100 ms	ernal-2.(eth3)	
0.050 ms		
0.000 ms	Naw	
litter		
Sittor		
0.022 ms	Average	N/A
Boy	pnVif.1 (bvpn1)	

 SD-WAN reporting page in Firebox System Manager

Settings						>
Traffic Monitor	Bandwidth Meter	SD-WAN	Service	Watch	Traffic Management	
Performance Me	tric Loss	 Graph 	Scale A	uto-Sca	le	~
- Color Sottings			Cus	stom Sc	ale	
Show				H	Hide	
BovpnVif.1 In	terface					
BovpnVif.2 In External Inter	iterface rface		Add <<			
Trusted Inter	face					
External-2 In	terface		> Remove			
Background		Te	xt Color		Grid Line 🔳	
Help					OK	Colors

Link Monitor Enhancements



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

Link Monitor — Enhancements

- Link Monitor has these enhancements:
 - You can now add Internal interfaces (Trusted, Optional, and Custom) and BOVPN virtual interfaces to Link Monitor
 - For example, you can monitor an internal interface that is used for a private network link such as an MPLS connection, private line, or leased line
 - You can now select to monitor single WAN interfaces in Link Monitor
 - Link Monitor is not enabled by default for interfaces

- In the Link Monitor configuration, now only monitored interfaces appear
 - Monitored interfaces are interfaces for which a target is configured
 - For example, if the interface External-2 does not have a Link Monitor target, External-2 does not appear in the Link Monitor interfaces list
- When you configure a new interface on the Firebox, Link Monitor is not automatically enabled for that interface
 - For example, if you add a new External interface, you must manually add that interface to Link Monitor
 - For External interfaces, we recommend that you configure a target other than the default gateway

Interfaces list in Link Monitor

🔣 Network Configuration									×
Interfaces Link Aggregation Bridge VLA	AN Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPoE	
Link Monitor Configuration	Settings: Specify the action with routing tab Next he Select the replaced. (e next hope for {0} I this interface can le will be used to for op:	. This is pref be routed to orward prob e status of {(ault gateway	erred so that the the next hop. If ing traffic and tr 0}. If you add cu target is used.	probing trat the next hop affic using S stom targets	ffic and traffic o is not specifie D-WAN action , the default ge	using an S ed, the norr with this ir ateway tar	D-WAN nal Iterface. get is	
		Туре		Target	Measure L	.oss, Latency,	a Ad	dd dit elete	
Add Delete	Require Use these Probe Deactivat	e a successful prote e settings for {0}: Interval: 5 e After: 3 e After: 3	 be to all targe Seconds Consecutive Consecutive 	ets to define the s utive Failures utive Successes	interface as	active.			
						<u>о</u> к с	<u>a</u> ncel	<u>H</u> elp	

- To configure a target for an interface, you must first add the interface to the Link Monitor interfaces list
- Add an interface to the list of monitored interfaces

Network	c Configuration										>	×		
Interfaces	Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPoE			
.ink Monito Monitored	r Configuration d Interfaces:			ettings:										
				Specify the action with routing tab Next he Select the replaced.	e next hope for {0} n this interface car le will be used to to op: targets to verify th Otherwise, the def	A. This is pref be routed to forward prob estatus of { fault gateway	ferred so that the the next hop. If the next h	probing traft the next hop affic using SI stom targets,	fic and traffic is not specific D-WAN action the default ga	using an SI ed, the norm with this in ateway targ	D-WAN hal terface. get is			
					Туре		🧝 Select an li	iterface to l	Monitor					
							N	ame		Туре	,		Zone	
				Require	a successful pro	be to all ta	1	ame	All	Туре	•	~	Zone	~
				Require Use these	a successful pro	be to all ta	External-2	ame	All	Туре	•	~	Zone All External	~
				Require Use these	a successful pro	be to all ta	External-2 BovpnVif.1	ame	All Physica BOVPN	Type al Virtual Inte	erface	~	Zone All External	~
				Require Use these Probe	a successful pro e settings for {0}: Interval: 5	be to all ta	External-2 BovpnVif.1 Trusted	ame	All Physica BOVPN Physica	Type al Virtual Inte al	erface	~	Zone All External Trusted	~
				Require Use these Probe Deactivat	a successful pro settings for {0}: Interval: 5 e After: 3	be to all ta	External-2 BovpnVif.1 Trusted MPLS	ame	All Physica BOVPN Physica Physica	Type al Virtual Inte al	erface	~	Zone All External Trusted Trusted	~
	_			Require Use these Probe Deactivat Reactivat	e a successful pro e settings for {0}: - Interval: 5 e After: 3 e After: 3	be to all ta	External-2 BovpnVif.1 Trusted MPLS External-1	ame	All Physica BOVPN Physica Physica Physica	Type al Virtual Inte al al	erface	· ·	Zone All External Trusted Trusted External	~
Add				Require Use these Probe Deactivat Reactivat	e a successful pro e settings for {0}: Interval: 5 e After: 3 e After: 3	be to all ta	External-2 BovpnVif.1 Trusted MPLS External-1	ame	All Physica BOVPN Physica Physica	Type al Virtual Inte al al	erface	•	Zone All External Trusted Trusted External	~

- Only the interfaces you add appear in the list
- To remove monitoring for an interface, you can delete the interface from the Link Monitor interfaces list

Link Monitor Configuration Monitored Interfaces: External-1 Specify the next hope for External-1. This is preferred so that the probing traffic an	
Monitored Interfaces: Settings: Specify the next hope for External-1. This is preferred so that the probing traffic an	
External-1 Specify the next hope for External-1. This is preferred so that the probing traffic an	
SD-WAN action with this interface can be routed to the next hop. If the next hop is m normal routing table will be used to forward probing traffic and traffic using SD-WAN interface. Next hop: Select the targets to verify the status of External-1. If you add custom targets, the of	of ramic using an ot specified, the action with this efault gateway
target is replaced. Otherwise, the default gateway target is used. Type Target Measure Loss, Latency,	Add
Ping 4.2.2.1	Edit
Ping 8.8.8.8 ()	
	Delete
Require a successful probe to all targets to define the interface as active.	
Use these settings for External-1:	
Probe Interval: 5 Seconds	
Deactivate After: 3 Consecutive Failures	

Link Monitor — Internal Interfaces

 When you add a Trusted, Custom, or Optional interface to Link Monitor, you must specify either a next hop IP address or a custom target

🔣 Network	Configuration										×
Interfaces	Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPoE
Link Monitor Monitored BovpnV MPLS	r Configuration I Interfaces: 'if.1		Se	ttings: Specify the SD-WAN ac normal routi interface Next ho Select the ti is replaced.	next hope for MPI ction with this inter ing table will be use p: 10.0.2 argets to verify the Otherwise, the de	LS. This is pr face can be r ed to forward .2 status of MI fault gatewa	eferred so that i routed to the nex d probing traffic PLS. If you add y target is used.	the probing to thop. If the and traffic u custom targe	raffic and traff next hop is not sing SD-WAN ets, the default	ic using an t specified, action with gateway ta	the this arget
				Туре	e Tar	get	Measure Lo	ss, Latency,	and Jitter	Add.	
				Ping	Next Hop	(Edit	
										Delet	e
				Require Use these Probe Ir Deactivate	a successful prob settings for MPLS nterval: 5 After: 3	e to all targets	s to define the ir ive Failures	iterface as a	ictive.		
Add	Delete			Reactivate	After: 3	Consecut	ive Successes				
								<u>0</u> I	۲ C <u>a</u> n	cel	<u>H</u> elp

Link Monitor — Internal Interfaces

- The next hop IP address tells the Firebox where to route:
 - Traffic to the link monitor target
 - Traffic that uses an SD-WAN action
- If you do not specify a next hop IP address for an internal interface, you must specify a custom target

nterfaces	Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPc
ink Monito Monitoreco MPLS BovpnV	r Configuration Interfaces:		Set	tings: Specify the SD-WAN ac normal routin Next hop Select the ta is replaced. Type	hext hope for MPL tion with this interf ing table will be use to see the second second second to second second second second second to second	.S. This is pr ace can be r ed to forward status of MI fault gatewa get	eferred so that t routed to the nex d probing traffic : PLS. If you add d y target is used. Measure Los	he probing tr t hop. If the r and traffic us custom targe ss, Latency, ;	affic and traff next hop is not sing SD-WAN a ts, the defau and Jitter	ic using an specified, t action with gateway ta	the this orget
Add Delete				Ping 4.2.2.1 Image: Consecutive Successes Image: Consecutive Successes Edit. Deleter Deleter Image: Consecutive Successes Edit.							;

Link Monitor — BOVPN Virtual Interfaces

- To monitor a BOVPN virtual interface, you must first:
 - Configure a virtual peer IP address in the BOVPN virtual interface settings
 - Use an IP address for the peer and not a netmask

Interface	erface] Assign virtual interface IP addresses (required for dynamic routing)								
Local IP address:	10. 0 . 49.1								
Peer IP address or netmask:	10. 0 . 50.1								
	Use a netmask for a VPN to a third-party endpoint. (Fireware OS v11.11 and higher)								
	<u>O</u> K C <u>a</u> ncel <u>H</u> elp								

Link Monitor — BOVPN Virtual Interfaces

- In Link Monitor, add the BOVPN virtual interface
 - A target to the virtual peer IP address is automatically configured
 - You cannot change or remove this target, and you cannot specify additional targets

🔣 Network Configuration								×		
Interfaces Link Aggregation Bridge	VLAN Loopbac	k Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN PPPo	E		
Link Monitor Configuration Monitored Interfaces: BovpnVif.1 Settings: Currently, for VPN VIE, we only support one type of probing target, by default, I.E. ping to pe										
MPLS	T	ype Ta Virtual Pe	rget er IP	Measure Loss, Latency, and Jitter			Add Edit			
				ha ia dafiaa iha	:-tf		Delete			
	Use the Prob Deactiv Reactiv	Require a successful probe to all targets to define the interface as active. Use these settings for BovpnVif.1: Probe Interval: 5 • Seconds Deactivate After: 3 • Consecutive Failures Reactivate After: 3 • Consecutive Successes								
Add Delete										
						<u>о</u> к С <u>я</u>	ancel <u>H</u> el	p		
Link Monitor — Single WAN Interfaces

- You can now monitor single WAN interfaces
 - In Policy Manager, this functionality was added in Fireware v12.4
 - In Web UI, this functionality was added in Fireware v12.3

nterfaces	Link Aggregation	Bridge	VLAN	Loopback	Bridge Protocols	WINS/DNS	Dynamic DNS	Multi-WAN	Link Monitor	SD-WAN	PPPoE
ink Monitor	r Configuration										
Monitored	Interfaces:		S	ettings:							
Externa				SD-WAN a normal rou interface. Next h Select the	e next hope for Ex action with this inte ting table will be us op:	rface can be sed to forwa	is preferred so t couted to the ne rd probing traffic xternal. If you	add custom t	argets, the def	ranic using ot specified I action with fault gatewa	, the h this ay
				target is re	eplaced. Otherwise	e, the default	gateway target	is used.			
				Тур	pe Ta	rget	Measure L	oss, Latency	/, and Jitter	Ad	ld
				Typ Ping	De Ta 203.0.113	3.1 (Measure L	oss, Latency	/, and Jitter	Ad Ed	ld it
				Typ Ping	De Ta 203.0.113	arget 3.1 (Measure L	oss, Latency	γ, and Jitter	Ed	ld it lete
				Ping Require	203.0.113 203.0.113 e a successful pro	be to all targe	Measure L	interface as	y, and Jitter	Ed De	ld it lete
				Typ Ping Require Use these	e a successful pro	be to all targe	Measure L	interface as	r, and Jitter	Ed De	ld it lete
				Ping Ping Require Use these Probe	e a successful pro e settings for Exter Interval: 5	be to all targer s.1 () be to all targer rnal: Second	Measure L	interface as	r, and Jitter	Ed De	ld it lete
				Ping Ping Require Use these Probe Deactivat	e a successful pro e settings for Exter Interval: 5 te After: 3	be to all targer Second Consec	Measure L ets to define the s utive Failures	interface as	r, and Jitter	Ed De	ld it lete

WatchGuard Training

Link Monitor — Interface Changes

- If an interface has Link Monitor targets but is not used by any SD-WAN actions:
 - If you disable the interface, Link Monitor is disabled automatically
 - For an internal interface, if you change the interface type to Bridge, VLAN, or Link Aggregation, Link Monitor is disabled automatically
 - Link Monitor is enabled automatically if you change a nonexternal interface to an external interface:
 - Interface type changed from internal to external
 - Interface type changed from Bridge, VLAN, or Link Aggregation to external



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- WebBlocker now includes a new Warn action
- Gives administrators more flexibility to enforce acceptable usage policies
- No longer need to block traffic that is borderline acceptable
- Increases employee awareness of policies in cases where the Deny action is too strict



 When users try to get access to a website in a WebBlocker category that has the Warn action assigned, a new warning page appears



- Users can click Continue to site to open the website or Go back to return to the previous page
- The warning page includes the WebBlocker category and cannot be customized

WatchGuard Training

- To assign the Warn action to a WebBlocker category:
 - 1. Edit a WebBlocker action
 - 2. In the **Categories** tab, select the category
 - 3. From the **Quick Action** drop-down list, select **Warn**
- To assign the Warn action to all uncategorized URLs:
 - 1. From the **When a URL is uncategorized** drop-down list, select **Warn**

lame:	Default-WebBlocker				
escription	Default configuration for	or WebBlocker			
Categories	Exceptions Advance	d Alarm Server			
Show all	categories 🗸 All Cate	egories v Search:		Quick Action	
Action	Category	Subcategory	Alarn	Quick Action	
Allow	Miscellaneous	Web Images	_	Allow	
Allow	Miscellaneous	Web Infrastructure		Warn	
Allow	News and Media	News and Media		Deny	
Allow	News and Media	Alternative Journals		Enable Alarm	
Deny	Parked Domain	Parked Domain		Disable Alarm	
Allow	Productivity	Productivity		Enable Logging	
Allow	Productivity	Advertisements		Disable Logging	
Allow	Productivity	Application and Software Download		Disable Logging	
Allow	Productivity	Instant Messaging			
Allow	Productivity	Message Boards and Forums			
Allow	Productivity	Online Brokerage and Trading			
Allow	Productivity	Pay-to-Surf			
Allow	Religion	Religion		\checkmark	
Allow	Religion	Non-Traditional Religions		\checkmark	
Allow	Religion	Traditional Religions		\checkmark	
Deny	Security	Security			
Deny	Security	Advanced Malware Command and Co.	[
Deny	Security	Bot Networks			
Deny	Security	Compromised Websites			
Deny	Security	Keyloggers			
Deny	Security	Malicious Embedded iFrame			
Deny	Security	Malicious Embedded Link			
Deny	Security	Malicious Web Sites			
Deny	Security	Mobile Malware			
Denv	Security	Phishing and Other Frauds			1
When a UI	RL is uncategorized Wa	rn 🗸 🗌 Alarm 🗹 Log this action	n		

- In HTTPS proxy actions, you can perform content inspection on WebBlocker categories with the Warn action
- Select the check box in the **Inspect** column
- When you do not enable content inspection, the HTTPS proxy allows categories with the Warn action and the Warn message does not appear

<u>N</u> ame: I	Default-H	TTPS-Client			
cription:	Created b	y Web UI QSW on 2019-01-15	T23:23:30-00:00		
ategories -					
Content Insp	pection	WebBlocker			
VebBlocker	r	10000000			
General Set	ttings				
-		WebBlocker: Default-V	/ebBlocker 🗸 📝 🖹	•	
		To inspect an allowed W	ebBlocker category, select the corresponding	check box. (Fireware OS v	11.9.4 and higher)
		Show all categories \sim	All Categories \lor Search:		Quick Action
		Category	Subcategory	Action	Inspect
		Social Web - Twitter	Social Web - Twitter	Allow	
		Social Web - YouTube	Social Web - YouTube	Allow	
		Society and Lifestyles	Society and Lifestyles	Allow	
		Society and Lifestyles	Alcohol and Tobacco	Allow	
		Society and Lifestyles	Blogs and Personal Sites	Allow	
		Society and Lifestyles	Gay or Lesbian or Bisexual Interest	Allow	
		Society and Lifestyles	Hobbies	Allow	
		Society and Lifestyles	Personals and Dating	Allow	
		Society and Lifestyles	Restaurants and Dining	Allow	
		Society and Lifestyles	Social Networking	Allow	
		Special Events	Special Events	Allow	
		Sports	Sports	Warn	
		Sports	Sport Hunting and Gun Clubs	Allow	
		Tasteless	Tasteless	Allow	님
		Travel	Travel	Allow	님
		Vehicles	Vehicles	Allow	님
		Violence	Violence	Allow	님
		Weapons	Weapons	Allow	
		Log this action	Inspect when a URL is uncategorized	Proxy Action: Default-HTT	TP-Client v
		Import Expor	t		

Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

When users try to get access to a website in a WebBlocker category that has the Warn action assigned, the Firebox writes a log message that includes the text **ProxyWarn**:

2019-03-15 15:42:38 Allow 10.0.1.2 34.232.27.44 http/tcp 50111 80 1-Trusted 0-External **ProxyWarn: HTTP Request categories** (HTTP-proxy-00) Default-HTTP-Client proc_id="http-proxy" rc="602" msg_id="1AFF-0021" proxy_act="Default-HTTP-Client" cats="Sports" op="GET" dstname="www.espn.com" arg="/favicon.ico" geo_dst="USA" Traffic:

- When you assign the Warn action to a WebBlocker category, the WG-Auth-WebBlocker policy is added to the configuration automatically
- This is the same policy that is added automatically when you enable the WebBlocker local override feature

Fitter: None Poil Policy Type From To Port cy Any-Trusted, Any-Optional Any-External tcp:21 xxy Any-Trusted, Any-Optional Any-External tcp:30 roxy Any-Trusted, Any-Optional Any-External tcp:413 Any-Trusted, Any-Optional Firebox tcp:4100 Any-Trusted, Any-Optional Firebox tcp:4100
Policy Type From To Port cy Any-Trusted, Any-Optional Any-External tcp:21 xyy Any-Trusted, Any-Optional Any-External tcp:30 roxy Any-Trusted Any-External tcp:43 Any-Trusted, Any-Optional Firebox tcp:4100 1 Any-Trusted, Any-Optional Firebox tcp:4100
cy Any-Trusted, Any-Optional Any-External tcp:21 xxy Any-Trusted, Any-Optional Any-External tcp:30 roxy Any-Trusted, Any-Optional Any-External tcp:443 Any-Trusted, Any-Optional Firebox tcp:4100 Any-Trusted, Any-Optional Firebox tcp:4100
oxy Any-Trusted, Any-Optional Any-External tcp:80 iroxy Any-Trusted Any-External tcp:443 Any-Trusted, Any-Optional Firebox tcp:4100 i Any-Trusted, Any-Optional Firebox tcp:4100
Invoxy Any-Trusted Any-External tcp:443 Any-Trusted, Any-Optional Firebox tcp:4100 Any-Trusted, Any-Optional Firebox tcp:4100
Any-Trusted, Any-Optional Firebox tcp:4100 h Any-Trusted, Any-Optional Firebox tcp:4100
h Any-Trusted, Any-Optional Firebox tcp:4100
tal Any-Trusted, Any-Optional Firebox tcp:4126
ware-XTM-WebUI Any-Trusted, Any-Optional Firebox tcp:8080
Any-Trusted, Any-Optional Any icmp (type: 8, code: 255)
Any-Trusted, Any-Optional Any-External tcp:53 udp:53
hox_Mamt Any_Trusted Any_Ontional Firebox top:4105 top:4117 top:4113
Any-Trusted, Any-Optional Any-External tcp:0 (Any) udp:0 (Any)
Any-Trusted, Any-Optional Any-External tcp:0 (Any) udp:0 (Any)
Any-Trusted, Any-Optional Any-External tcp:0 (Any) udp:0 (Any)
Ware-XTM-VVEDUI Any-Trusted, Any-Optional Prebox tcp:su Any-Trusted, Any-Optional Any icmp (1 Any-Trusted, Any-Optional Any-External tcp:53 hox.Momt Any-Trusted Any-Optional Firebox tcp:41

- If the Firebox uses a self-signed certificate for authentication, users will receive a certificate warning for the new warning page
- To resolve this, install a trusted certificate on the Firebox, or import the self-signed certificate on each client device

DNSWatch in Bridge Mode



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

Firebox supports DNSWatch in Bridge Mode

- Can only be configured in Web UI, not CLI or WatchGuard System Manager
- Prerequisite Firebox system IP address must be able to connect to the DNSWatch Server
 - This system IP address is the source IP address in DNS request packets redirected to the DNSWatch DNS server
- Provides the same types of information as Mixed Routing Mode but is called Global Bridge
- Known Issue Local domains can't be resolved even when a local DNS server is specified
 - Workaround Create DNS Forwarding Rules for local domains

IPv6 Support for BOVPN and BOVPN Virtual Interfaces



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- You can now create VPN tunnels directly between two IPv6 addresses
 - Tunneling over IPv4 is not required
- If an ISP provides only IPv6 addresses, you can now continue to deploy
 Fireboxes in those environments



- BOVPN and BOVPN virtual interface configurations now support IPv6
- In the Address Family drop-down list, if you select IPv6 Addresses, you must specify an IPv6 address for all other BOVPN settings that require an IP address

ewa	ay Name:	gateway.1							
Iress	s Family:	IPv6 Addre	esses				 ✓ (Fire 	eware OS	v12.4 or higher)
		IPv4 Addre	sses						
enera	al Settings	Pv6 Addre	sses						
Cred	lential Metl	hod							
Οι	Use Pre-S	hared Key							
Οı	Use IPSec	Firebox Cer	tificate						
Sele	ect the cer	rtificate to be	used for	the Gateway					
Id			Certif	icate Name				Algorith	m
	Show All	Certificates							
	Show All	Certificates							
Gate	Show All	Certificates	al Gatewa	y.		Remote Ga	teway		Add
Gater #	Show All	certificates	al Gatewa	y ID	IP Address	Remote Ga	teway		Add
Gater #	Show All	Certificates	al Gatewa	y D	IP Address	Remote Ga	teway		Add Edit
Gate	Show All	certificates	al Gatewa	y D	IP Address	Remote Ga	teway D		Add Edit Delete
Gate	Show All	certificates	al Gatewa	y ID	IP Address	Remote Ga	teway ID		Add Edit Delete
Gate	Show All	e Type	al Gatewa	y ID	IP Address	Remote Ga	teway		Add Edit Delete Move up
Gater	Show All	Certificates points Loc e Type	al Gatewa	y D	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down
Gate	Show All	Certificates points Loc e Type	al Gatewa	y D	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down
Gater	Show All	Certificates points Loci e Type	al Gatewa	y D	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down
Gate	Show All	Certificates	al Gatewa	y D	IP Address	Remote Ga	teway ID		Add Edit Delete Move up Move down
Gate [™]	Show All	Certificates	al Gatewa	y D	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down
Gate #	Show All	m for failove	al Gatewa r	y D hox starts	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down
3ate #	Show All	m for failove	al Gatewa r rhen Fireb	y D hox starts	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down

 The interface you select for the local gateway must have a static IPv6 interface IP address, or the interface must be enabled as a DHCPv6 client

Interface Settings - Interface # 4	×
IPv4 IPv6 Secondary MAC Access Control Advanced	^
Enable IPv6 Static IPv6 Addresses	
IP Address	Add
2001:db8::1/64	Edit
	Delete
🔣 🔣 🔣 🔣	teway Endpoints Settings - BovpnVif.4
A tunnel need details for the Local Gate Interface:	eds authentication on each side of the tunnel. Provide the configuration e gateway endpoints below. eway
Physi	ical External-2 ~
O Other	r Select
Interface	e IP Address 2001:db8::1

- These BOVPN and BOVPN virtual interface settings are not supported for IPv6 tunnels:
 - Multicast
 - Modem failover
 - NAT and direction
 - Broadcast routing
 - Attempt to resolve domain setting

Syslog Servers





Support for Multiple Syslog Servers

 You can now configure a Firebox to send log messages to a maximum of three syslog servers

Send log	WSM Log , message	Server es to these Dime	ension or WSM Log S	Servers:		
Log Ser	rvers 1	Log Servers 2				
The serve	Vers VOU S	pecify on the L	og Servers 2 tab a	re only available f	for	
	cra you a					
devices v	with Firev	vare OS v11.10) and higher.			Configure
devices v Syslog Server	with Firew	vare OS v11.10) and higher.			Configure
devices v Syslog Server	with Firew r message	vare OS v11.10) and higher. og servers:			Configure
devices v Syslog Server ✓ Send log	with Firew r message	vare OS v11.10 es to these sysl	og servers:	Description		Configure
devices v Syslog Server	with Firew r I message ress	vare OS v11.10 es to these syst	og servers:	Description		Configure
devices v Syslog Server ✓ Send log	with Firew r I message ess	Port	og servers: Log Format Syslog	Description Server 1	^	Add Edit
Syslog Server Send log	r message 0 0	Port 514 544	og servers: Log Format Syslog Syslog	Description Server 1 Server 2	^	Add Edit
Syslog Server ✓ Send log IP Addre 10.0.1.30 10.0.2.30 10.0.3.30	r message 0 0 0	vare OS v11.10 es to these syst Port 514 514	og servers: Log Format Syslog Syslog Syslog	Description Server 1 Server 2 Server 3		Add Edit Remove
Syslog Server Syslog Server Send log IP Addre 10.0.1.30 10.0.3.30 i Mu Firebox Interne	r message iono iono iono iono iono iono iono ion	Port 514 514 10g servers are	og servers: Log Format Syslog Syslog Syslog e supported in Firewa	Description Server 1 Server 2 Server 3 are OS v12.4 and	higher	Configure Add Edit Remove r.
Syslog Server Send log IP Addre 10.0.1.30 10.0.3.30 i Mu Firebox Interna Send log	r message 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Port 514 514 514 514 sog servers are e	and higher. og servers: Log Format Syslog Syslog e supported in Firewa ernal storage	Description Server 1 Server 2 Server 3 are OS v12.4 and	higher	Configure Add Edit Remove r.

Ę

Proxy Support for TLS 1.3



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

Proxy Support for TLS 1.3

- Fireware now supports TLS 1.3 protocol
- Provides compliance and support for the latest standards
- Allows full inspection of HTTPS traffic
- TLS 1.3 connections are now supported and not downgraded to TLS 1.2



Proxy Support for TLS 1.3

- These proxies now support the TLS 1.3 protocol:
 - HTTPS
 - SMTP
 - IMAP
 - POP3
- Proxies no longer support the SSL v3 protocol. When SSL v3 protocol is specified by the client:
 - Connections are now denied immediately
 - Proxies do not allow negotiation to a different protocol

TLS Profile Updates

- Minimum Protocol Version changes
 - TLS v1.2 added
 - SSLv3 removed
- When you upgrade to Fireware v12.4, any existing TLS Profiles with SSLv3 as the Minimum Protocol Version are updated to use TLS v1.0 automatically



TLS Profile Updates

- TLS 1.3 always uses Perfect Forward Secrecy (PFS) Ciphers
- If you select None from the Perfect Forward Secrecy Ciphers drop-down list:
 - TLS 1.3 is disabled for proxy content inspection negotiation
 - TLS v1.2 and below can be negotiated based on Client/Server support and the Minimum Protocol Version in the TLS profile





WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

 An enhanced FireCluster Diagnostics page shows you more details upfront with better organization





Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- This information now appears on the main FireCluster Diagnostics page:
 - Cluster mode (active/passive or active/active)
 - Cluster ID

F

- Detailed information is now organized in three tabs:
 - Diagnostics Heartbeat, interface up/down status, health indexes, and more
 - File Objects Sync status of objects such as the password, license, and signatures
 - Event History A list of past cluster events

- A status indicator on each tab lets you know whether a cluster member requires attention:
 - If the indicator is green, the cluster functionality is normal
 - If the indicator is red, one or more cluster issues are present
 - To find an issue, look for a red status indicator in each tab section. For example, if the Hardware Health Index has a value considered as unhealthy, the Health section of the Diagnostics tab has a red indicator

Main page and **Diagnostic** tab

						30 SECONDS 🔻
reCluster						
ireCluster						
Synchronized						
Cluster enabled for: 1d 1h 13m 40s	MEMBER ROLE	SERIAL NUMBER	STATUS	UPTIME	CPU	MEMORY
Cluster Mode- active-passive	Master	801002DAA2FEB	Online	1h 18m 6s	0%	29%
	Backup	801002DFD1C29	Online	1h 15m 7s	0%	27%
Cluster ID: 118						
Connections: 55						
Connections per second: 0						
More Details						
NOI E Details						
X Diagnostic V File Object Event His	tory					
K Backup - 801002DFD1C29						
✓ FireCluster State		🗸 Health	h			More Deta
Heartbeat: Yes		S	vstem Health Index:	100		
Management Interface: Up		Monitored	Ports Health Index:	100		
Primary Cluster Interface: Up			Weighed Avg Index:	100		
× Monitored Interfaces	More Detail	s Runtime	Objects			
eth0: Up			BOVPN Tunnels:	0		
eth1: Up			CONNTRACK:	10		
eth10: Down						
eth11: Down						

WatchGuard Training

File Object tab

ireCluster								30 SECONDS *
ireCluster								
 Synchronized 								
Cluster enabled f	for: 1d 1h 16m	0s	MEMBER ROLE	SERIAL	STATUS	UPTIME	CPU	MEMORY
Cluster Mor	de: active-pass	sive	Master	801002DAA2FEB	Online	1h 20m 26s	0%	29%
Cluster	ID: 118		Bachun	801002DED1C20	Online	1h 17m 27e	09/	279/
Connectio	ns: 32		backup	8010020701029	Olimie	10 1/00 2/5	0.16	27.70
Connections per seco	nd 1							
More Det	alle							
More Dea	ans							
More Deu	8115							
X Disensatic	File Object	Event History						
X Diagnostic	File Object	Event History						
X Diagnostic	File Object	Event History						
X Diagnostic	File Object	Event History						
Viagnostic File Objects Configuration: Password:	File Object Matched Matched	Event History						
Diagnostic File Objects Configuration: Password: Certificate:	File Object Matched Matched Matched	Event History						
Viagnostic File Objects Configuration: Password: Certificate: License:	File Object Matched Matched Matched Matched	Event History						
Diagnostic File Objects Configuration: Password: Certificate: License: IPS Signature:	File Object Matched Matched Matched Matched Matched Matched	Event History						
Viagnostic File Objects Configuration: Password: Certificate: License: IPS Signature: GAV Signature:	File Object Matched Matched Matched Matched Matched Matched Matched	Event History						
Vignostic File Objects Configuration: Password: Certificate: License: IPS Signature: GAV Signature: IAV Signature:	File Object Matched Matched Matched Matched Matched Matched Matched Matched	Event History						
Vignostic File Objects Configuration: Password: Certificate: License: IPS Signature: GAV Signature: IAV Signature: DLP Signature: DLP Signature:	File Object Matched Matched Matched Matched Matched Matched Matched Matched Matched	Event History						
★ Diagnostic ✓ File Objects Configuration: Password: Certificate: License: IPS Signature: GAV Signature: IAV Signature: DLP Signature: Botnet:	File Object Matched Matched Matched Matched Matched Matched Matched Matched Matched Matched	Event History						
Diagnostic File Objects Configuration: Password: Certificate: License: IPS Signature: GAV Signature: IAV Signature: DLP Signature: Botnet: Geolocation:	File Object Matched Matched Matched Matched Matched Matched Matched Matched Matched Matched Matched Matched	Event History						

WatchGuard Training

Event History tab

FireCluster							30 SECONDS ▼
FireCluster							
✓ Synchronized							
Cluster enabled for:	1d 1h 16m 20s	MEMBER RO	LE SERIAL N	UMBER STATUS	UPTIME	CPU	MEMORY
Cluster Mode:	active-passive	Master	801002DA	A2FEB Online	1h 20m 46s	0%	29%
Cluster ID:	118	Backup	801002DF	D1C29 Online	1h 17m 47s	0%	27%
Connections:	26						
Connections per second:	0						
More Details							
🗙 Diagnostic 🗸 F	ile Object Event History						
Cluster Member Histo	DrV LAST 7 DAYS						
Failovers:	0	CLUSTER ST	ATUS	PERCENTAG	E	TIME	
Faults:	0	Both Member	s Up	100.000%		7d 0h 0m	
Cluster Downtime:	0d 0h 0m	Single Membe	er Up	0.000%		Od Oh Om	
		Both Member	s Down	0.000%		0d 0h 0m	
History from 2019-01-18 12:00:00) AM to 2019-01-25 10:33:20 AM						
12 PM Sat 19 12 F	PM Jan 20 12 PM	Mon 21 12	PM Tue 22	12 PM Wed 2	23 12 PM Thu 2	24 12 PM	Fri 25
DATE ≑		EVENT	RE	ASON		DURATI	ON

WatchGuard Training

Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

- The More Details link in each section shows you a list of associated events.
 - For example, if you click the More Details link in the Monitored Interfaces section, you see a list of interface events ("Interface Up" and "Interface Down")

More Details link

🗙 Diagnostic 🧹 File Obj	ect Event History					
× Backup - 801002DFD1	.C29					
✓ FireCluster State						
Heartbeat:	Yes					
Management Interface: Primary Cluster Interface:	Up Up					
× Monitored Interface	S	м	ore Details			
eth0:	Up					
eth1: eth10:	Down					
eth11:	Down		Master 801002D	A2FEB - Mor	nitored Interfaces	
			DATE ≑	INTERFACE	DESCRIPTION	
			2019-01-25 09:13:04	eth7	Interface UP	
			2019-01-25 09:14:25	eth7	Physical link down	

2019-01-25 09:15:19

2019-01-25 09:15:41

2019-01-25 09:15:57

eth7

eth7

eth7

Interface UP

Interface UP

Physical link down

CLOSE

Geolocation Deny Message



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

Geolocation Deny Message

- A new *Deny* message now appears when Geolocation blocks access to a website
- In previous releases, the connection would timeout



 The message includes the name of the blocked country and cannot be customized

Exception/Blocked Site List Enhancements



WatchGuard Training Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved
Exceptions/Blocked Site List Enhancements

- In Fireware Web UI and CLI, you can now add IP addresses, Network IP address ranges, and Host IP address ranges that overlap to these lists:
 - Blocked Sites
 - Blocked Sites Exceptions
 - Botnet Site Exceptions
 - Geolocation Exceptions
 - RADIUS SSO Exceptions
- This feature was already supported in Policy Manager
- Domain names that overlap are not allowed

Exceptions/Blocked Site List Enhancements

- For example, you can now add these exceptions to a Geolocation action:
 - Host IPv4: 10.0.0.1
 - Network IPv4: 10.0.0/24

Geolocation / Edit Geolocation Contr	rol Action				
Geolocation Control Action Settings					
Name Global	Description Pre-defin	ied system default			
Select the countries to block by geogra	Select the countries to block by geographic location. Geolocation prevents connections to and from the countries you specify.				
Map Country List E	xceptions				
Geolocation Exceptions					
IP ADDRESS		DESCRIPTION			
10.0.0.1					
10.0.0/24					
ADD REMOVE IMPORT	EXPORT				
SAVE CANCEL					

Synchronize Feature Key Enhancements



Synchronize Feature Key Enhancements

- If Automatic Feature Key Synchronization is enabled, the Firebox now automatically synchronizes the feature key after you:
 - Restore a Backup Image (with or without Fireware OS)
 - Upgrade Fireware OS
 - Downgrade Fireware OS
- Benefits:
 - Makes sure the feature key includes support for new features after you upgrade
 - Updates the feature key if you restore a backup image that includes an expired license

	 LiveSecurity Service 	Unlimited	Jun 3, 2021
	Network Discovery	Unlimited	Jun 3, 2021
	Reputation Enabled Defense	Unlimited	Jun 3, 2021
	✓ spamBlocker	Unlimited	Jun 3, 2021
	Threat Detection & Response	Unlimited	Jun 3, 2021
	VebBlocker	Unlimited	Jun 3, 2021
	Concurrent Session Maximum	100000	Never
	Total Number of Authenticated Users	500	Never
	Total Number of VLAN Interfaces	50	Never
	Branch Office VPN Tunnels	40	Never
Ire	L2TP Users	25	Never
	V IPSec VPN Users	25	Never
			1
tor new	Enable automatic feature key synchronization (Firew	are OS v11.6.	3 and higher)
	Send alarm notification when feature key is going to	oe expired or I	nas been exp
arada	(Fireware OS v11.10.1 and higher)		
grauc			
-			
Leave of Leave			
Kev It voll			
			-

Summary

Model:

Serial Number

Signature

Features

Feature

Software Edition

Gateway AntiVirus (AV)

Intrusion Prevention (IPS

Dimension Command

Data Loss Prevention

DNSWatch

T35-W

D0640338599D9

302D021501A76E6C-62385B59064A3472-D920C021EA76E951-0C23841

Value

Unlimited

Unlimited

Unlimited

Unlimited

Unlimited

Status

869 days

869 davs

869 days

869 davs

869 days

869 days 869 days 869 days 869 days 869 days

869 days

Notifications.

Cancel

Help

Expiration

Jun 3, 2021

Fireware OS

Х

Import.

Download.

Remove

Details.

Proxy Enhancements for DNSWatch



Proxy Enhancements for DNSWatch

- When users try to get access to a domain on the DNSWatch Blackholed domain list:
 - The Firebox now treats the connection to the Blackhole Server educational page as a trusted host connection and allows it
 - The Firebox now writes a log message that includes this text:

ProxyDeny: HTTP DNSWatch blackholed domain

Proxy Enhancements for DNSWatch

 When a domain is in both the DNSWatch Blackholed Domain list and a denied WebBlocker category, the Blackhole Server page now appears instead of a WebBlocker Deny message



FQDN Limit Increase



FQDN Limit Increase

- You can now configure up to a total of 2048 Fully Qualified Domain Names (FQDNs) on these devices:
 - Firebox Cloud
 - FireboxV
 - M Series: M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600
 - T Series: T55, T55-W, T70
- All other devices continue to support up to 1024 FQDNs

MD5 in Gateway AV/IntelligentAV Logs



MD5 in Gateway AV and IntelligentAV Logs

 Gateway AntiVirus and IntelligentAV log messages now include the MD5 hash values of malicious and suspicious files

Gateway AntiVirus:

Nov 28 14:54:25 2018 M400 local1.info http-proxy[2674]: msg_id="1AFF-0028" Deny 1-Internal 0-External-1 tcp 10.0.1.106 100.100.100.121 60912 80 msg="ProxyDrop: HTTP Virus found" proxy_act="HTTP-Client.Standard.1" **md5="dea724a49e3ab3e0b0857150217fd743**" virus="WM.DMV.A" host="100.100.100.121" path="/gav/virus.doc" (HTTP-proxy-00)

IntelligentAV:

2018-11-28 15:06:09 Deny 10.0.1.106 100.100.100.121 http/tcp 60940 80 1-Internal 0-External-1 ProxyDrop: HTTP Virus found (HTTP-proxy-00) proc_id="http-proxy" rc="594" msg_id="1AFF-0028" proxy_act= "HTTP-Client.Standard.1" host="100.100.100.121" path="/iavtest/virus.doc" virus="malicious" md5="1c0bd146af6358ad929f3e4b2bd14f8d"

SSO Agent Debug Tool Enhancements



SSO Agent Debug Tool Enhancements

 Status detail now shows connection information to help you troubleshoot SSO issues

ebug Log :	On		Refresh Interval	5 sec	onds 💌	
SOagent version:	12.4.0.31059 B585506					
LM, EM and SSO cl	ient status:					
Domain Name	IP Address	Туре	Status	Versio	n	Build
		ELM EM	connected disconnected	12.3.1	.0	585506
		40.000 00-10 40.0				
withentication Info: S	uccess: 2. From ELM:2, EM	1:0, 550 Clienco, AD:0				
Domain Name	IP Address	Type	User Name	_	Authentication	Time
Domain Name ssofqdn.com	IP Address	Type ELM	User Name administrator		Authentication 1/22/2019 1:4	Time 0.04 PM
wthentication Info: S Domain Name ssofqdn.com ssofqdn.com	IP Address	ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2246 PM
uthentication Info: S Domain Name ssoligdin.com ssoligdin.com	IP Address	Type ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM 2.46 PM
uthentication links: S Domain Name ssoligdin.com ssoligdin.com roccessing IP list: 54 IP Address	IP Address IP Address IP Address Type	Type ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM ending IP list. 38 IP Address
uthentication Info: 5 Domain Name ssolgdn.com ssolgdn.com tocessing IP list: 54 IP Address 1.1.1.77	IP Address	Type ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM ending IP fist 38 IP Address • 1.1.2.2
uthentication Info: 5 Domain Name ssoligdn.com ssoligdn.com rocessing IP list: 54 IP Address 1.1.1.77 1.1.2.77	IP Address	Type ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM ending IP list: 38 IP Address 1.1.2.2 1.1.1.3
uthentication Info: S Domain Name ssoligdn.com ssoligdn.com 'nocessing IP list: 54 IP Address 1.1.1.277 1.1.1.78	IP Address	Type ELM ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM 2.46 PM IP Address 1.1.22 1.1.1.3 1.1.2.3
Notessing IP list: 54 IP Address 1.1.1.77 1.1.2.77 1.1.2.78	Type ELM ELM ELM ELM ELM	ELM	User Name administrator ssotest1		Authentication 1/22/2019 1:4 1/22/2019 2:2	Time 0.04 PM 2.46 PM 2.46 PM ending IP list: 38 IP Address 1.1.22 1.1.1.3 1.1.23 1.1.1.4

WatchGuard Training

SSO Agent Debug Tool Enhancements

- Connection information:
 - ELM, EM, and SSO Client Status Connection status information
 - Authentication Info Success Information about current users who have successfully authenticated
 - Pending IP list Indicates requests sent to SSO Agent but not processed
 - Processing IP list The information request is in process with ELM, EM, SSO Client or Active Directory
 - **Refresh interval** is configurable for 5 second, 10 second, 30 second, 60 second, 2 minute, and 5 minute intervals

SSO Agent Debug Tool

- Provides easy visibility into the SSO authentication process
- Pending or Processing lists are usually empty because the requests typically process in less time than the refresh rate
- When a client tries to authenticate, the request is sent to the Firebox
- The Firebox forwards the request to the SSO Agent
- The request to the SSO Agent appears in the Pending IP List
 - If an IP address is in the Pending IP List, begin to investigate with the SSO Agent

SSO Agent Debug Tool

- When a request starts processing in ELM, EM, AD, or the SSO Client, the IP address appears in the Processing IP List
 - If an IP address is in the Processing IP List, look at the ELM, EM, AD, SSO Client, or SSO Agent
- When an IP has authenticated, it appears in the Authentication Info Success list until the user logs off

Access Portal Enhancements



Resize RDP Window Enhancement

- You can now resize the RDP window in your browser without reconnection issues
- The Automatic option resizes the RDP window smoothly instead of forcing you to reconnect and, sometimes, reauthenticate
- Added TLS 1.2 support for compliance with environments where TLS 1.0 is prevented
- Support for this feature is dependent on an OS that supports RDP 8.1

Operating Systems Supported

- Windows 7 with RDP 8.1 update
- Windows 8.1 and higher
- Windows Server 2012 R2 and higher

General	Session	Display		
Col	or Depth	24-bit (16 million colors)	•	
Resize	e Method	Automatic Automatic Disabled	 I, Windows Server 201 	2 R2,
		systems or ones that may have select "Disabled".	e issues with resizing the screen	eratin; ,
		select "Disabled".		

 Versions prior to Windows 8.1 or Windows Server 2012 R2 without RDP 8.1 updates must select **Disabled**

AD Domains Hidden

- Active Directory Domains are now hidden on the Access Portal sign-in page
- The first server in the Authentication Server list is the default server
- User who authenticate with a different server must add <domain>\ before their username to authenticate



RADIUS and SecurID support for IPv6 and 64-character shared secret



IPv6 Support for RADIUS and SecurID

 On the Firebox, you can now configure IPv6 addresses for RADIUS and SecurID servers in both Fireware Web UI and Policy Manager

Servers / RADIUS			
Before you configure your Firel server can successfully accept a	box device to use a RADIUS auti and process RADIUS authentica	nentication server, m tion requests.	ake sure th
Primary Server Settin	gs		
Enable RADIUS Server			
IP Address	2001:4860:4860::8888		
Port	1812		
Shared Secret			
Confirm Secret			
Timeout	10	seconds	
Retries	3		
Dead Time	3 Minutes	•	
Group Attribute	11		

Make sure that the Primary Server Se	users can	success	fully authen	ticate to the Se	curlD server.
Enable Secur	ID server	ickup Sei	ver Settinga	•	
IP Address:	2001:486	60:4860::8	3888		~
Port:				1812	÷
Shared Secret:					
Confirm Secret:					
Timeout:				10	seconds
Retry:				3	•
Dead Time				3	🔹 minutes 🗸
Group Attribute:				11	•

64-Character Shared Secret

 You can now use up to 64 characters in the shared secret for RADIUS and SecurID servers in both Fireware Web UI and Policy Manager

Servers / RADIUS		
Before you configure your Firel server can successfully accept	oox device to use a RADIUS authenticat and process RADIUS authentication req	ion server, make sure the uests.
Primary Server Settin	gs	
Enable RADIUS Server		
IP Address	2001:4860:4860::8888	
Port	1812	
Shared Secret		•
Confirm Secret		
Timeout	10	seconds
Retries	3	
Dead Time	3 Minutes v	
Group Attribute	11	

Authentication Servers	×
Firebox-DB RADIUS SecurID	LDAP Active Directory
Make sure that the users can se	uccessfully authenticate to the SecurID server.
Primary Server Settings Back	up Server Settings
Enable SecurID server	
IP Address: 2001:4860:	4860::8888 ~
Port:	1812 🜩
Shared Secret: ••••••	
Confirm Secret:	
Timeout:	10 🚔 seconds
Retry:	3 🔹
Dead Time	3 ➡ minutes ∨
Group Attribute:	11 🔦

Technology Integrations Page Updates



Updates to Technologies Integrations Page

New splash page for Technology Integrations

third party product at the same time.

Autotask[®]

ConnectWise

Tigerpaw

- **Configure** opens the partner configuration page
- Integration Guide opens the Online Help Integration Guide
- Learn More opens the partner page on WatchGuard.com
- Solution Brief opens a downloadable version of the solution
 brief
 Technology Integrations
 WatchGuard partners with industry-leading technology companies to develop tight integrations for stronger security, easier deployments, and better interoperability in your IT
 WatchGuard partners with industry-leading technology companies to develop tight integrations for stronger security, easier deployments, and better interoperability in your IT
 watchGuard partners with industry-leading technology companies to develop tight integrations for stronger security, easier deployments, and better interoperability in your IT

Autotask

Autotask Corporation helps IT organizations worldwide work smarter with a complete, cloud-based IT business management platform that enables efficiency, accountability and access to the metrics that drive intelligent business decisions.

Integration: WatchGuard Firebox appliances integrate with Autotask PSA for integrated, closed-loop service ticketing and auto synchronization of asset information.



ConnectWise

Made for companies that sell, service, and support technology, ConnectWise is the leading business management platform worldwide that enables technology companies to achieve the highest level of profitability and service to their clients.

Integration: WatchGuard Firebox appliances and WatchGuard Dimension integrate with ConnectWise for service ticketing, security asset synchronization, and automated reporting directly from ConnectWise.

Tigerpaw

Tigerpaw deliver complete business automation and management across all aspects of your business: organizing and streamlining operations, building a marketing and sales pipeline, optimizing your customer's experience and understanding your metrics.

Integration: WatchGuard Firebox appliances integrate with Tigerpaw PSA for integrated, closed-loop service ticketing and auto synchronization of asset information.

CONFIGURE INTEGRATION GUIDE

Device Configuration Template Updates



Device Configuration Template – QoS

- In a Device Configuration Template on the Management Server, you can now configure QoS settings
 - Supported in templates for Fireware 12.0 or higher
- Before you can configure QoS in a policy, you must enable all traffic management and QoS features in the Global Settings

Global Settings
Device Feedback Device feedback includes performance data that helps WatchGuard improve products and features. Th feedback does not include personally identifiable or organizationally identifiable information. Details Send device feedback to WatchGuard
Fault Report Fault reports include logs, core dumps, configuration files, and similar information that helps WatchGua troubleshoot errors and implement product improvement initiatives such as bug fixes. Details Send Fault Reports to WatchGuard daily
Traffic Management and QoS
Traffic generated by the Firebox (Fireware OS v12.2 and higher) Enable configuration of policies for traffic generated by the Firebox (Fireware OS v12.2 and higher)
OK Cancel Helr

Device Configuration Template – QoS

- When the global setting is enabled, you can configure QoS on the Advanced tab in a firewall policy
- QoS settings in a Device Configuration Template are the same as in an individual Firebox configuration

New Policy Properties		
me: FTP-proxy		🗹 Enab
Policy Properties Advanced		
Schedule: Always Or	n 🗸 🛐 🕒	
Traffic Management Actions	- Tali Dafault (Ila Limita)	
Porward (From		
Reverse (10 >	From). Derauli (No Limits)	
Connection Rate (per second)		
No Limit		\sim
Alarm when capacity excer	eded N	lotification
10110 5		
ICMP Error Handling	10112 0 11	
Use global setting	 ICMP Setting 	
QoS		
Override per-interface setting	gs	
Marking Type:	DSCP	~
marking type.		-
Marking Method:	Preserve	\sim
Value:	0 (Best Effort)	\sim
Prioritize Traffic Based On:	Custom Value	\sim
Value	0 (blormal)	~
value.	o (Normal)	

Device Configuration Template – DNS/WINS

- In a Device Configuration Template on the Management Server, you can now configure DNS/WINS settings
 - Supported in templates for Fireware 12.0 or higher
- To specify DNS and WINS settings, edit the Device Configuration Template, and select Setup > DNS/WINS

R DNS/WINS			>
DNS (Domain Name S Domain Name: DNS Servers:	ystem) Servers		
	Add	Edit	Remove
WINS (Windows Inter	net Naming Servic	e) Servers	
WINS Servers:			
		OK	Cancel

Device Configuration Template – DNS/WINS

- In the Inheritance Settings, the Other list now includes System DNS/WINS Settings
- To control inheritance of these settings, select or clear the Allow Override check box

Policies	Other			
Policy Types				
Schedules	Allow Override	Settings		
Aliases		Geolocation (Fireware US V11.12 and higher)		
Proxy Actions		Global Firewall Authentication settings		
Content Actions		Intrusion Prevention settings		
TLS Profiles		Mobile Security (Fireware US V11.11 and higher)		
HTTPS Exception Overrides		NTP Settings		
Application Control		Policy Filters		
Geolocation Control		Policy Tags		
Data Loss Prevention		Quarantine Server settings		
WebBlockers		Deputation Enabled Defense feedback settings		
Traffic Management		Send log messages to Firebox internal storage		
SNAT		Send log messages when the configuration for this device is		
Authentication Servers		Signature Update settings		
Authorized Users / Groups		Single Sign-On settings		
Quotas Rule		SNMP Settings		
Quotas Action		spamBlocker settings		
Other		Sysing Server		
		System DNS/WINS Settings		
		Torning Control Collinge		
	\checkmark	Threat Detection & Response (Fireware OS v11.12 and high		
	\checkmark	Tigerpaw Settings (Fireware OS v12.3 and higher)		
	\checkmark	Traffic Management and QoS Settings		
	\checkmark	WatchGuard Log Server settings		
	\checkmark	WebBlocker Settings (Fireware OS v11.12 and higher)		
	<	>		
	Select All	Unselect All		

Device Configuration Template – WebBlocker

- Device Configuration
 Templates now support the WebBlocker Warn action
- Supported for Fireware v12.4 and higher

Name:	newWebBlocker.1				
Description:	Default configuration for Wel	Blocker			
Categories	Exceptions Advanced Ala	arm Server			
Show all ca	ategories 🗸 🗸 All Categories	s v Search:		Quick Action	\sim
Action	Category	Subcategory	Alarm	Log	
Allow	Education	Reference Materials		\checkmark	- A
Allow	Entertainment	Entertainment		\checkmark	
Allow	Entertainment	Media File Download		\checkmark	
Allow	Extended Protection	Extended Protection		\checkmark	
Allow	Extended Protection	Dynamic DNS		\checkmark	
Allow	Extended Protection	Elevated Exposure		\checkmark	
Allow	Extended Protection	Emerging Exploits		\checkmark	
Allow	Extended Protection	Newly Registered Websites		\checkmark	
Allow	Extended Protection	Suspicious Content		\checkmark	
Allow	Gambling	Gambling		\checkmark	
Allow	Games	Games		\checkmark	
Allow	Government	Government		\checkmark	
Allow	Government	Military		\checkmark	
Allow	Government	Political Organizations		\checkmark	
Allow	Health	Health		\checkmark	
Allow	Illegal or Questionable	Illegal or Questionable		\checkmark	
Allow	Information Technology	Information Technology		\checkmark	
Allow	Information Technology	Computer Security		\checkmark	
Allow	Information Technology	Hacking		\checkmark	
Allow	Information Technology	Proxy Avoidance		\checkmark	
Allow	Information Technology	Search Engines and Portals		\checkmark	
Allow	Information Technology	Unauthorized Mobile Marketplaces		\checkmark	
Allow	Information Technology	Web Analytics		\checkmark	
Allow	Information Technology	Web and Email Marketing		\checkmark	
Allow	Information Technology	Web and Email Spam		\checkmark	\sim
When a URI Note: Warn	L is uncategorized Warn v	Alarm I Log this action			

Edit 1-to-1 NAT



Edit 1-to-1 NAT

You can now edit a 1-to-1 NAT configuration in the Web UI



Thank You!



