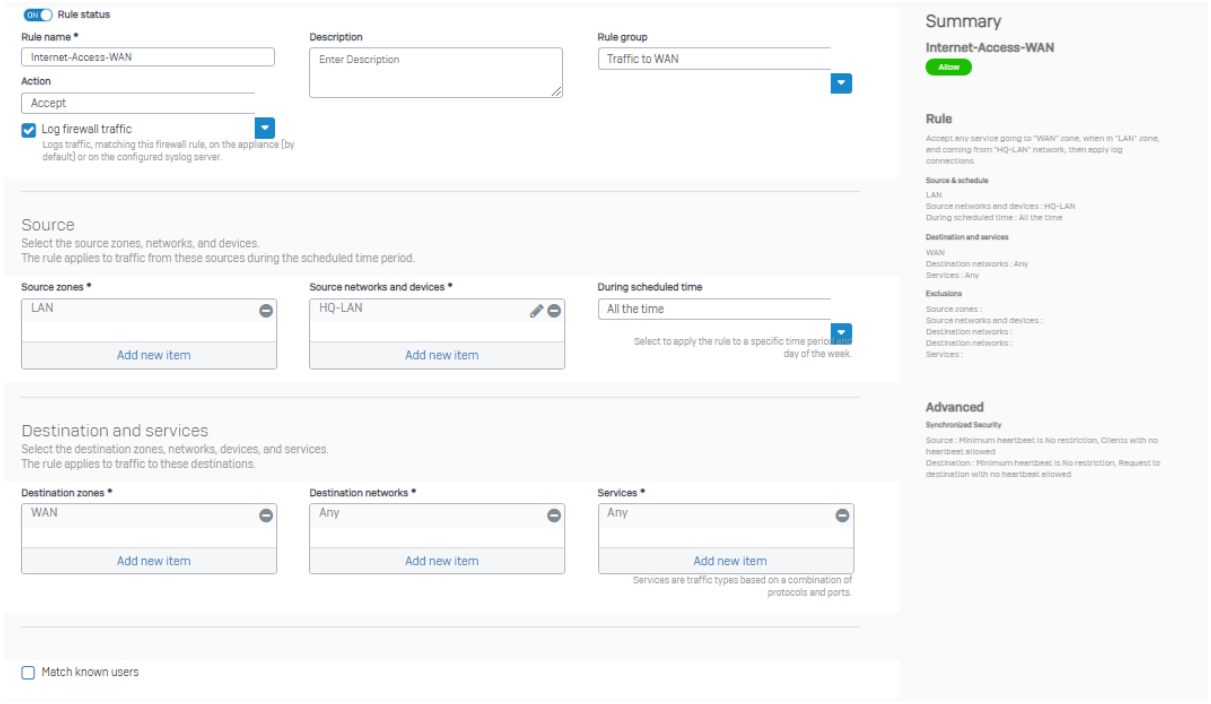
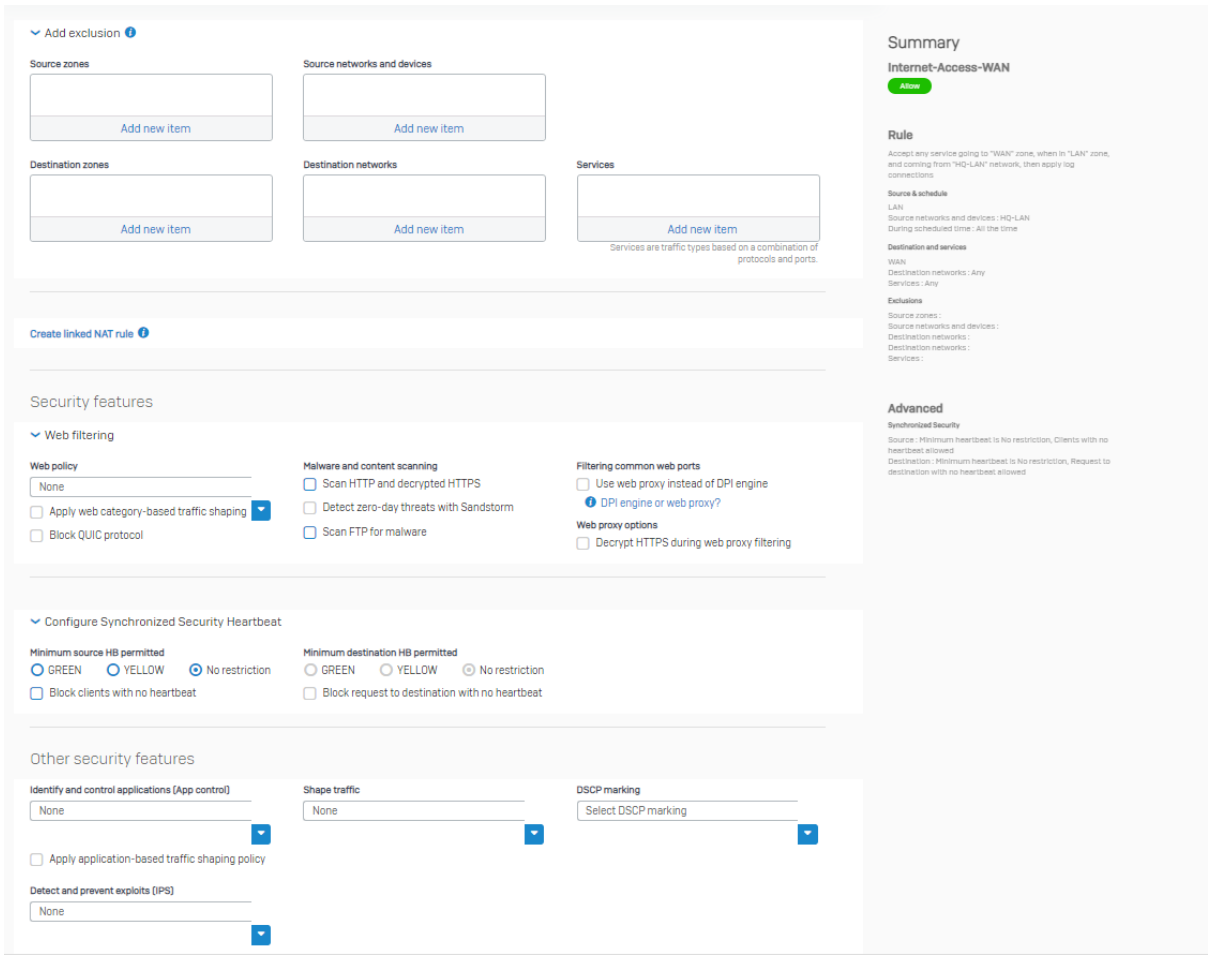

ON
Rule status
Rule name *
Internet-Access-WAN
Description
Enter Description
Rule group
Traffic to WAN
Action
Accept
Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.
Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.
Source zones *
LAN
Add new item
Source networks and devices *
HQ-LAN
Add new item
During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.
Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.
Destination zones *
WAN
Add new item
Destination networks *
Any
Add new item
Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports.
Match known users
Summary
Internet-Access-WAN
Allow
Rule
Accept any service going to "WAN" zone, when in "LAN" zone, and coming from "HQ-LAN" network, then apply log connections
Source & schedule
LAN
Source networks and devices : HQ-LAN
During scheduled time : All the time
Destination and services
WAN
Destination networks : Any
Services : Any
Exclusions
Source zones :
Source networks and devices :
Destination networks :
Destination networks :
Services :
Advanced
Synchronized Security
Source : Minimum heartbeat is No restriction, Clients with no heartbeat allowed
Destination : Minimum heartbeat is No restriction, Request to destination with no heartbeat allowed


Add exclusion
Source zones
Add new item
Source networks and devices
Add new item
Destination zones
Add new item
Destination networks
Add new item
Services
Add new item
Services are traffic types based on a combination of protocols and ports.
Create linked NAT rule
Security features
Web filtering
Web policy
None
Apply web category-based traffic shaping
Block QUIC protocol
Malware and content scanning
Scan HTTP and decrypted HTTPS
Detect zero-day threats with Sandstorm
Scan FTP for malware
Filtering common web ports
Use web proxy instead of DPI engine
DPI engine or web proxy?
Web proxy options
Decrypt HTTPS during web proxy filtering
Configure Synchronized Security Heartbeat
Minimum source HB permitted
GREEN
YELLOW
No restriction
Block clients with no heartbeat
Minimum destination HB permitted
GREEN
YELLOW
No restriction
Block request to destination with no heartbeat
Other security features
Identify and control applications (App control)
None
Apply application-based traffic shaping policy
Detect and prevent exploits (IPS)
None
Shape traffic
None
DSCP marking
Select DSCP marking
Summary
Internet-Access-WAN
Allow
Rule
Accept any service going to "WAN" zone, when in "LAN" zone, and coming from "HQ-LAN" network, then apply log connections
Source & schedule
LAN
Source networks and devices : HQ-LAN
During scheduled time : All the time
Destination and services
WAN
Destination networks : Any
Services : Any
Exclusions
Source zones :
Source networks and devices :
Destination networks :
Destination networks :
Services :
Advanced
Synchronized Security
Source : Minimum heartbeat is No restriction, Clients with no heartbeat allowed
Destination : Minimum heartbeat is No restriction, Request to destination with no heartbeat allowed