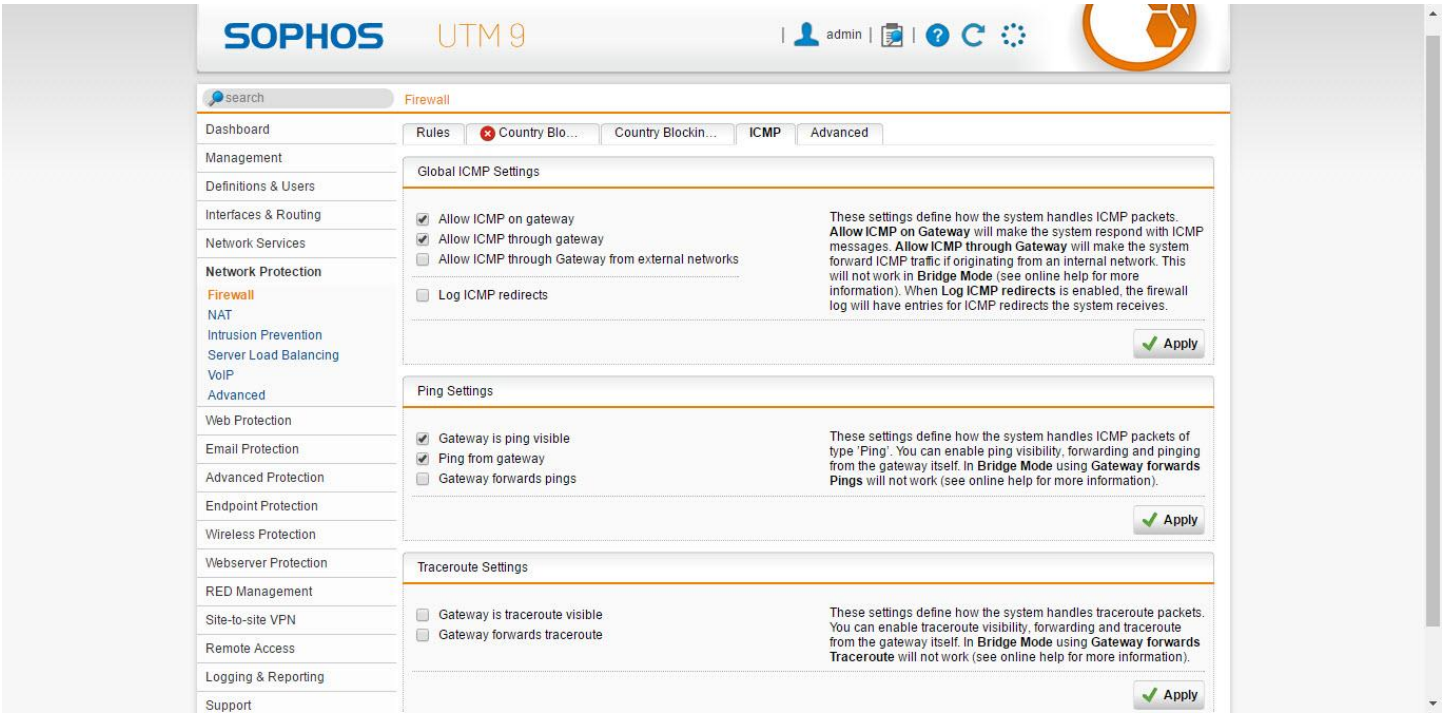
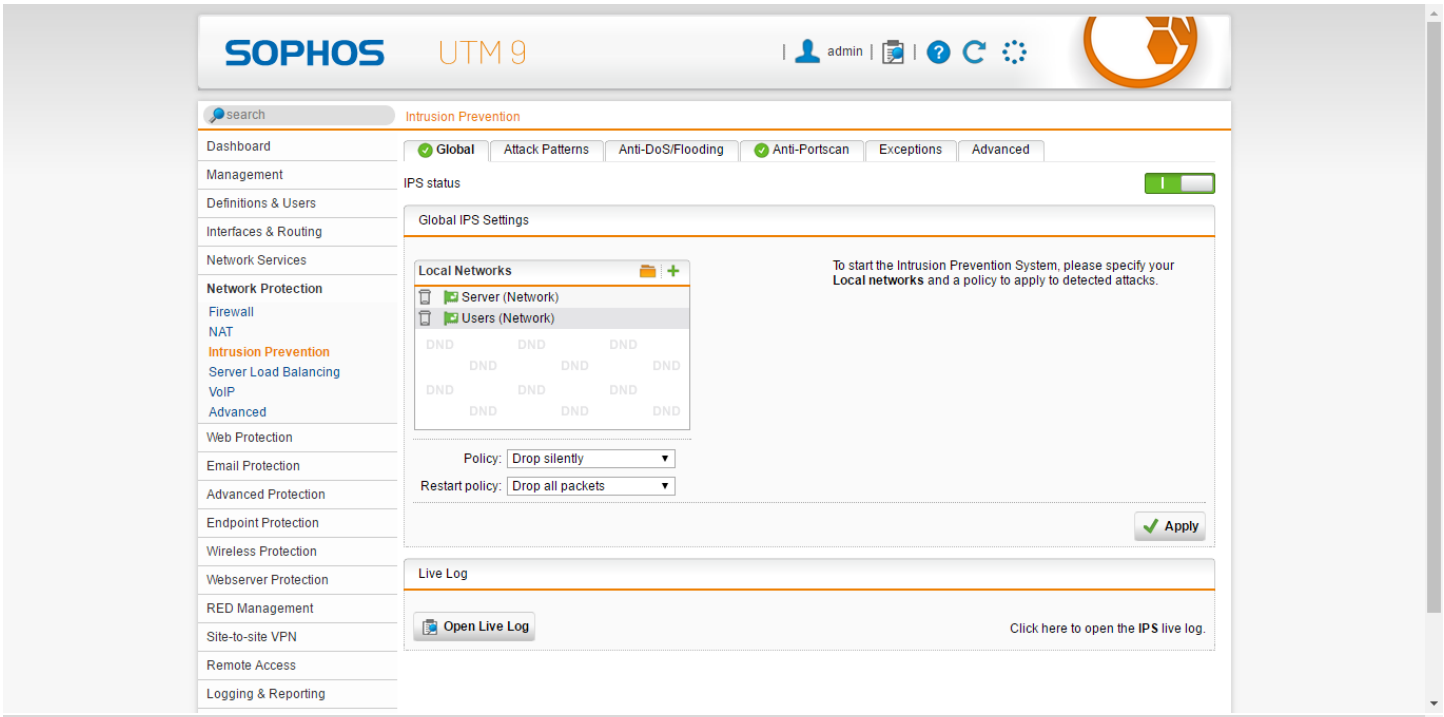
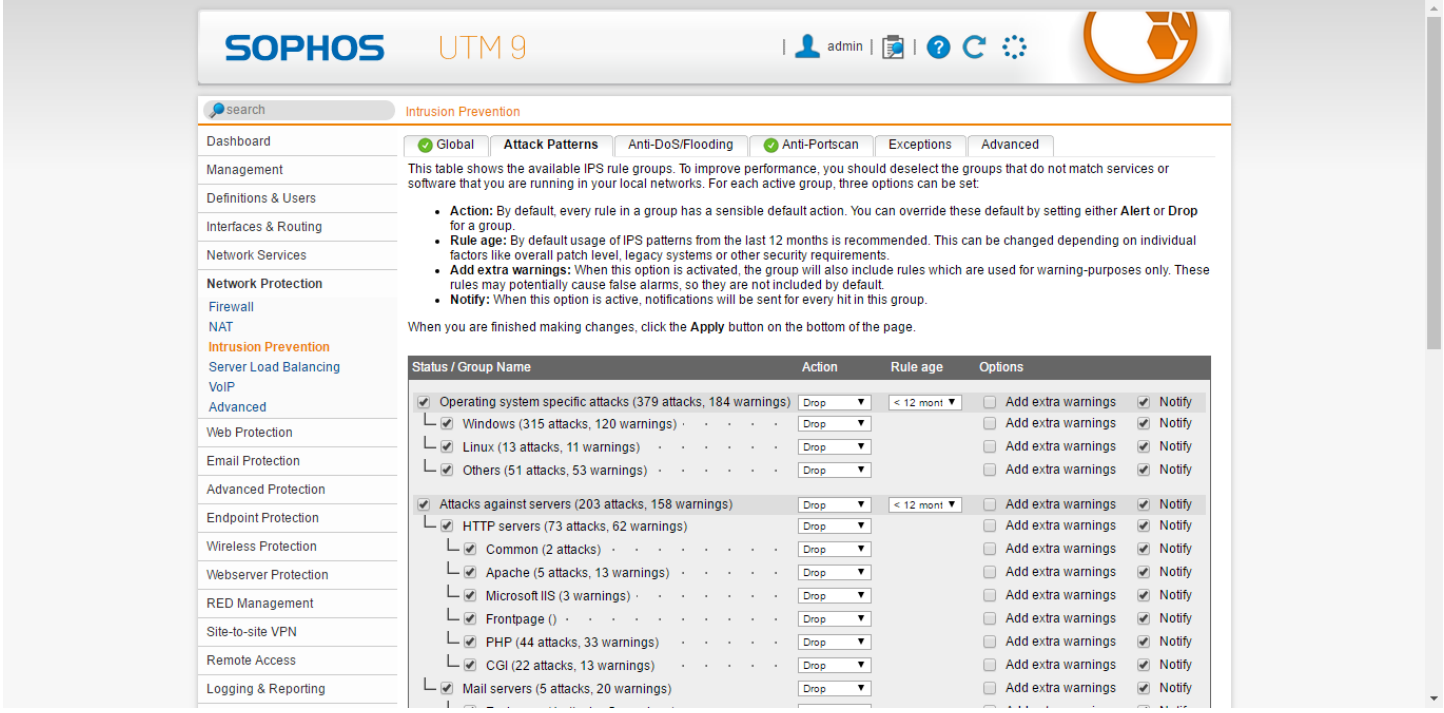
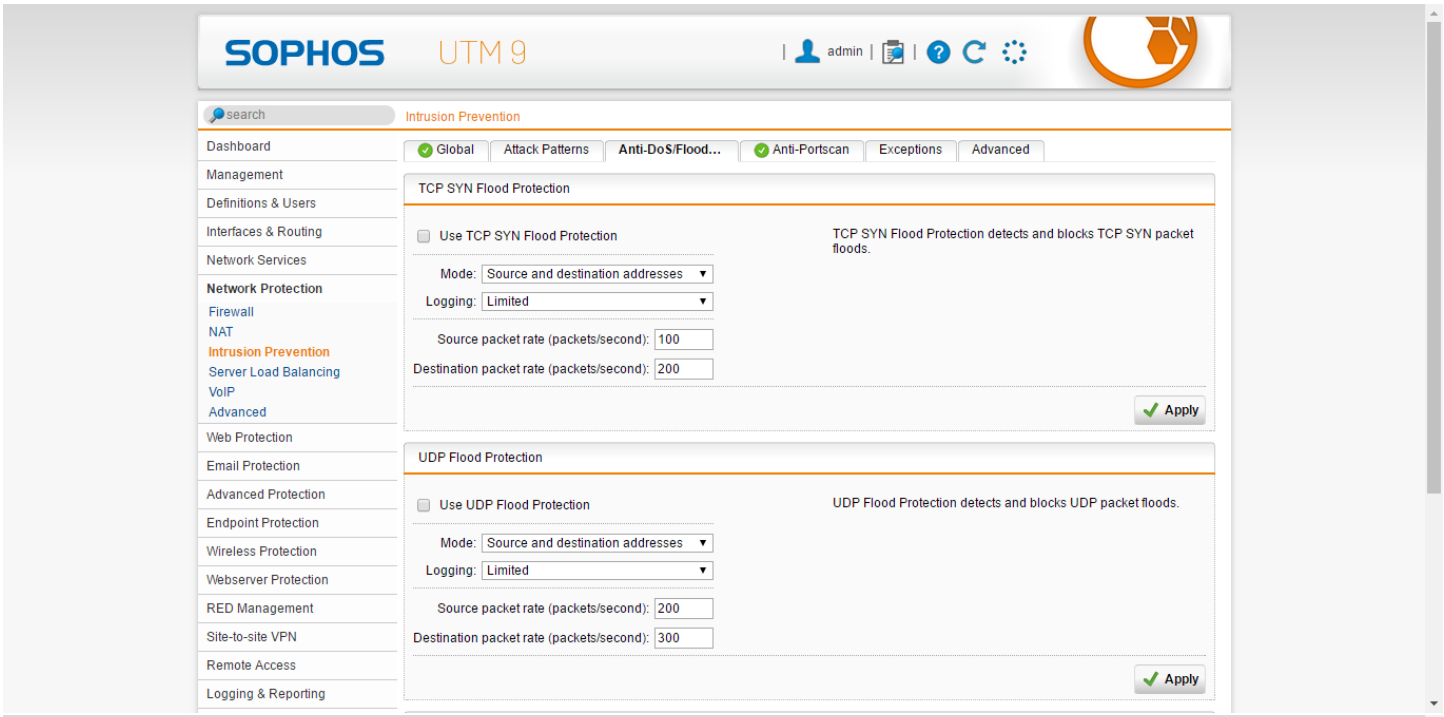
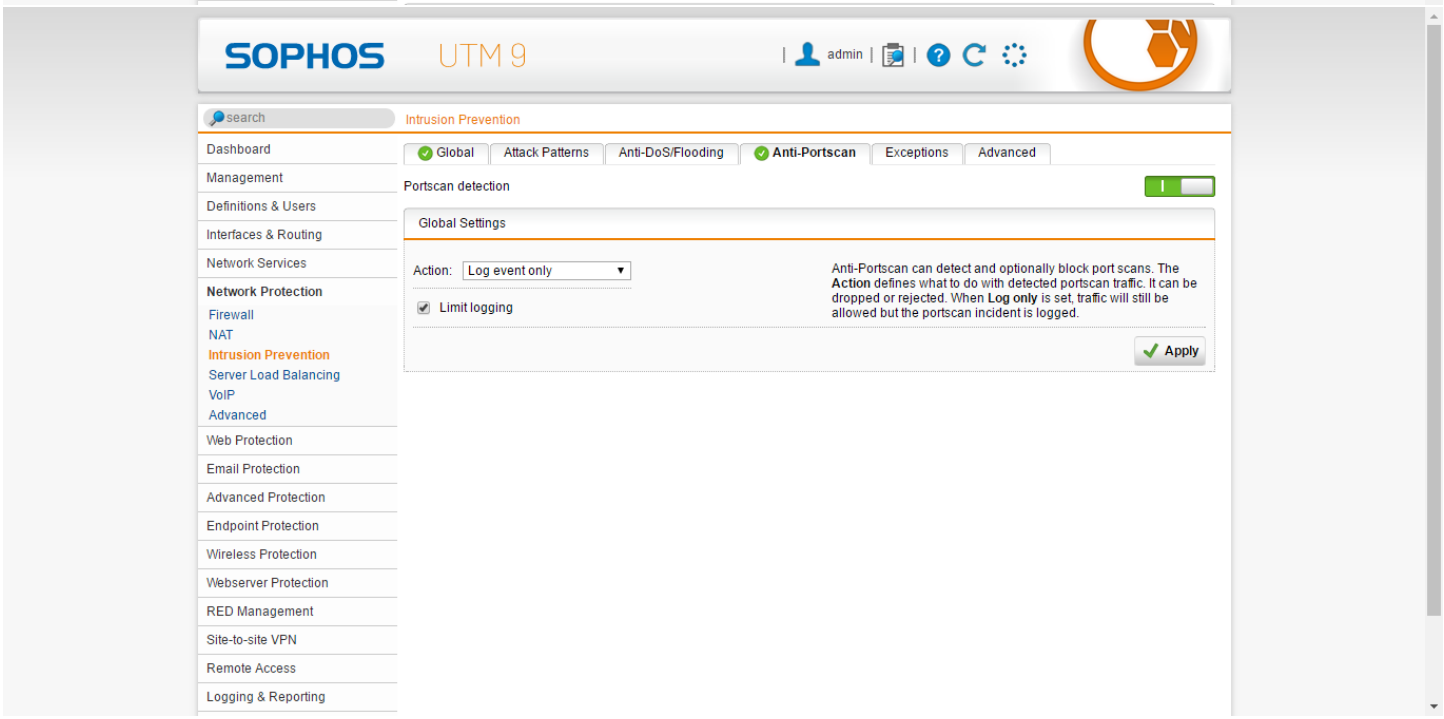
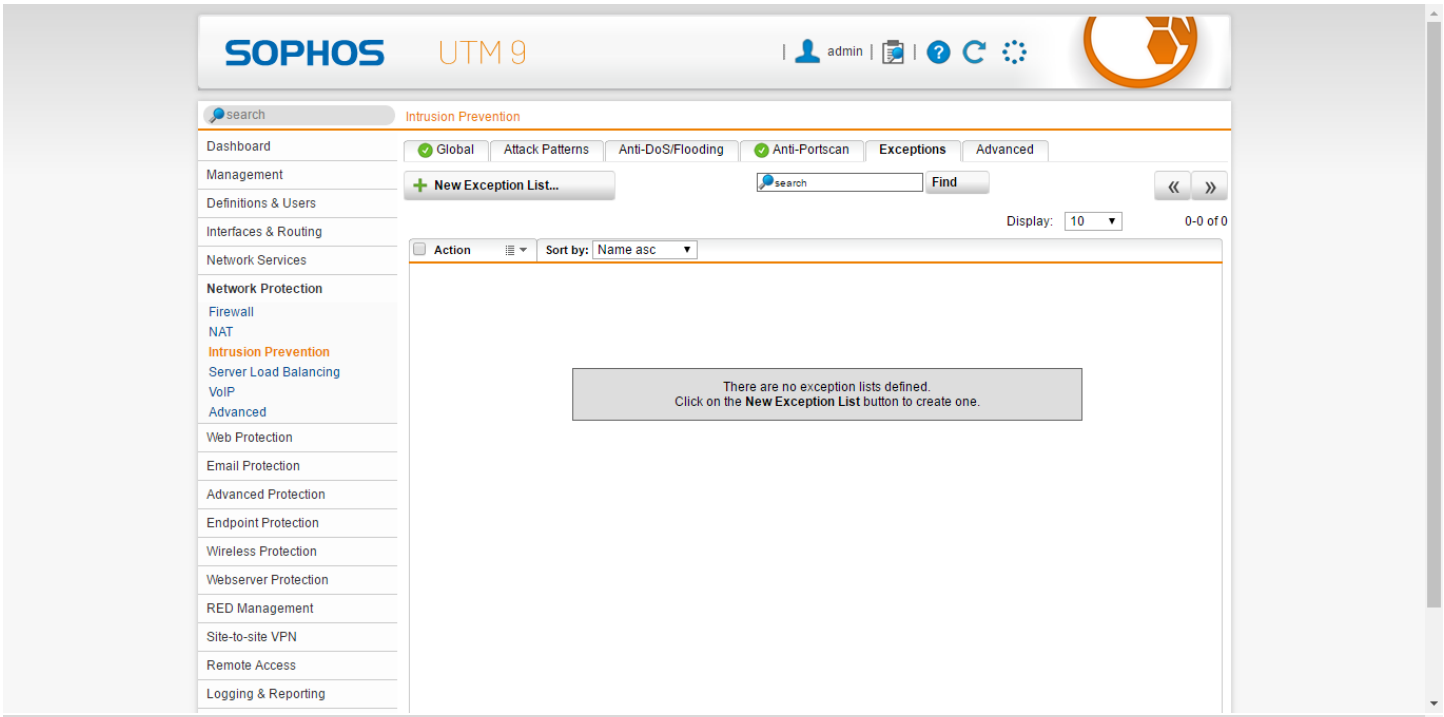

SOPHOS UTM 9
admin
search
Firewall
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Support
Rules
Country Blo...
Country Blockin...
ICMP
Advanced
Global ICMP Settings
Allow ICMP on gateway
Allow ICMP through gateway
Allow ICMP through Gateway from external networks
Log ICMP redirects
These settings define how the system handles ICMP packets. Allow ICMP on Gateway will make the system respond with ICMP messages. Allow ICMP through Gateway will make the system forward ICMP traffic if originating from an internal network. This will not work in Bridge Mode (see online help for more information). When Log ICMP redirects is enabled, the firewall log will have entries for ICMP redirects the system receives.
Apply
Ping Settings
Gateway is ping visible
Ping from gateway
Gateway forwards pings
These settings define how the system handles ICMP packets of type 'Ping'. You can enable ping visibility, forwarding and pinging from the gateway itself. In Bridge Mode using Gateway forwards Pings will not work (see online help for more information).
Apply
Traceroute Settings
Gateway is traceroute visible
Gateway forwards traceroute
These settings define how the system handles traceroute packets. You can enable traceroute visibility, forwarding and traceroute from the gateway itself. In Bridge Mode using Gateway forwards Traceroute will not work (see online help for more information).
Apply

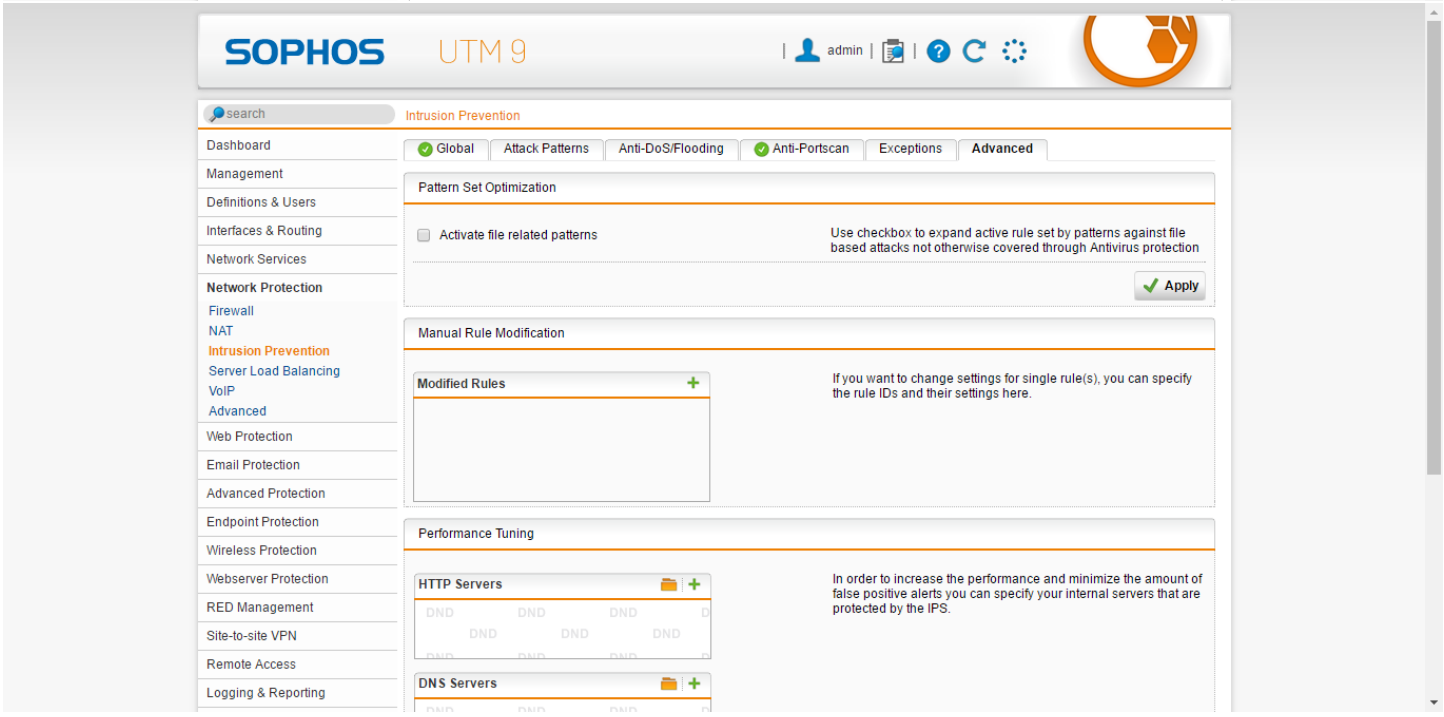

SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flooding
Anti-Portscan
Exceptions
Advanced
IPS status
Global IPS Settings
Local Networks
Server (Network)
Users (Network)
To start the Intrusion Prevention System, please specify your Local networks and a policy to apply to detected attacks.
Policy: Drop silently
Restart policy: Drop all packets
Apply
Live Log
Open Live Log
Click here to open the IPS live log.

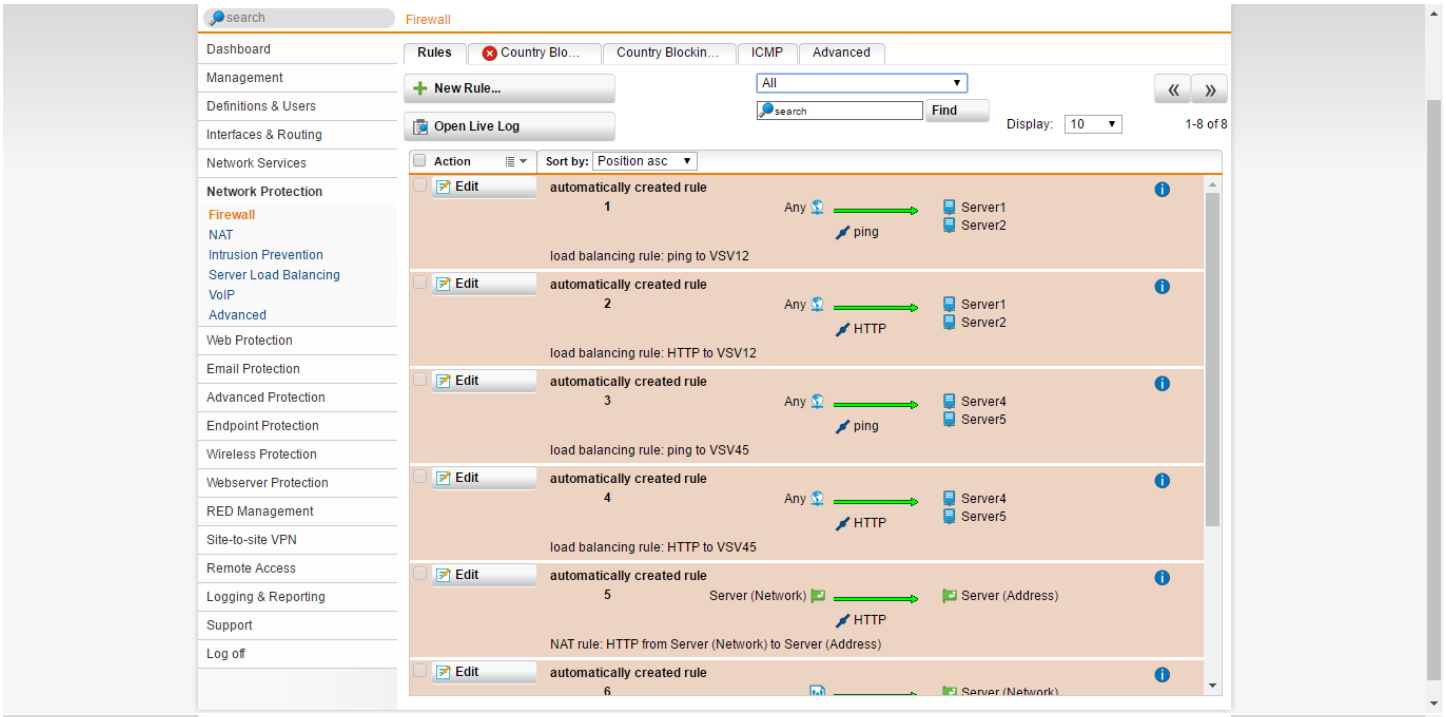

SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flooding
Anti-Portscan
Exceptions
Advanced
This table shows the available IPS rule groups. To improve performance, you should deselect the groups that do not match services or software that you are running in your local networks. For each active group, three options can be set:
Action: By default, every rule in a group has a sensible default action. You can override these default by setting either Alert or Drop for a group.
Rule age: By default usage of IPS patterns from the last 12 months is recommended. This can be changed depending on individual factors like overall patch level, legacy systems or other security requirements.
Add extra warnings: When this option is activated, the group will also include rules which are used for warning-purposes only. These rules may potentially cause false alarms, so they are not included by default.
Notify: When this option is active, notifications will be sent for every hit in this group.
When you are finished making changes, click the Apply button on the bottom of the page.
Status / Group Name
Action
Rule age
Options
Operating system specific attacks (379 attacks, 184 warnings)
Windows (315 attacks, 120 warnings)
Linux (13 attacks, 11 warnings)
Others (51 attacks, 53 warnings)
Attacks against servers (203 attacks, 158 warnings)
HTTP servers (73 attacks, 62 warnings)
Common (2 attacks)
Apache (5 attacks, 13 warnings)
Microsoft IIS (3 warnings)
Frontpage ()
PHP (44 attacks, 33 warnings)
CGI (22 attacks, 13 warnings)
Mail servers (5 attacks, 20 warnings)
Drop
< 12 mont
Add extra warnings
Notify

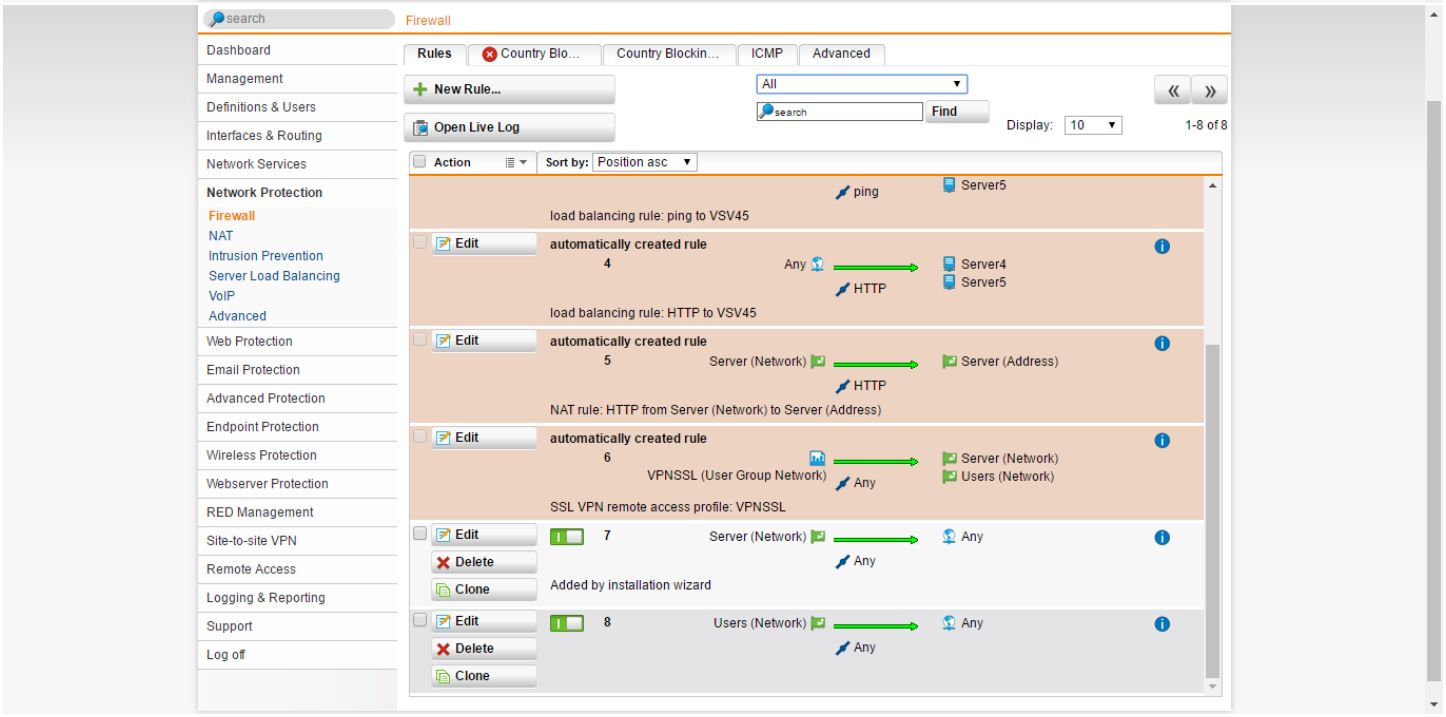

SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flood...
Anti-Portscan
Exceptions
Advanced
TCP SYN Flood Protection
Use TCP SYN Flood Protection
TCP SYN Flood Protection detects and blocks TCP SYN packet floods.
Mode: Source and destination addresses
Logging: Limited
Source packet rate (packets/second): 100
Destination packet rate (packets/second): 200
Apply
UDP Flood Protection
Use UDP Flood Protection
UDP Flood Protection detects and blocks UDP packet floods.
Mode: Source and destination addresses
Logging: Limited
Source packet rate (packets/second): 200
Destination packet rate (packets/second): 300
Apply


SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flooding
Anti-Portscan
Exceptions
Advanced
Portscan detection
Global Settings
Action: Log event only
Limit logging
Anti-Portscan can detect and optionally block port scans. The Action defines what to do with detected portscan traffic. It can be dropped or rejected. When Log only is set, traffic will still be allowed but the portscan incident is logged.
Apply


SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flooding
Anti-Portscan
Exceptions
Advanced
New Exception List...
search
Find
Display: 10
0-0 of 0
Action
Sort by: Name asc
There are no exception lists defined.
Click on the New Exception List button to create one.


SOPHOS UTM 9
admin
search
Intrusion Prevention
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Global
Attack Patterns
Anti-DoS/Flooding
Anti-Portscan
Exceptions
Advanced
Pattern Set Optimization
Activate file related patterns
Use checkbox to expand active rule set by patterns against file based attacks not otherwise covered through Antivirus protection
Apply
Manual Rule Modification
Modified Rules
If you want to change settings for single rule(s), you can specify the rule IDs and their settings here.
Performance Tuning
HTTP Servers
DND
In order to increase the performance and minimize the amount of false positive alerts you can specify your internal servers that are protected by the IPS.
DNS Servers


search
Firewall
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Support
Log off
Rules
Country Blo...
Country Blockin...
ICMP
Advanced
New Rule...
Open Live Log
All
search
Find
Display: 10
1-8 of 8
Action
Sort by: Position asc
Edit
automatically created rule
1
Any
ping
Server1
Server2
load balancing rule: ping to VSV12
automatically created rule
2
Any
HTTP
Server1
Server2
load balancing rule: HTTP to VSV12
automatically created rule
3
Any
ping
Server4
Server5
load balancing rule: ping to VSV45
automatically created rule
4
Any
HTTP
Server4
Server5
load balancing rule: HTTP to VSV45
automatically created rule
5
Server (Network)
HTTP
Server (Address)
NAT rule: HTTP from Server (Network) to Server (Address)
automatically created rule
6


search
Firewall
Dashboard
Management
Definitions & Users
Interfaces & Routing
Network Services
Network Protection
Firewall
NAT
Intrusion Prevention
Server Load Balancing
VoIP
Advanced
Web Protection
Email Protection
Advanced Protection
Endpoint Protection
Wireless Protection
Webserver Protection
RED Management
Site-to-site VPN
Remote Access
Logging & Reporting
Support
Log off
Rules
Country Blo...
Country Blockin...
ICMP
Advanced
New Rule...
Open Live Log
All
search
Find
Display: 10
1-8 of 8
Action
Sort by: Position asc
ping
Server5
load balancing rule: ping to VSV45
Edit
automatically created rule
4
Any
HTTP
Server4
Server5
load balancing rule: HTTP to VSV45
automatically created rule
5
Server (Network)
HTTP
Server (Address)
NAT rule: HTTP from Server (Network) to Server (Address)
automatically created rule
6
VPNSSL (User Group Network)
Any
Server (Network)
Users (Network)
SSL VPN remote access profile: VPNSSL
Edit
Delete
Clone
7
Server (Network)
Any
Any
Added by installation wizard
Edit
Delete
Clone
8
Users (Network)
Any
Any