

Standard +

Access Control

Policy

NAT

Threat Prevention

Custom Policy

Autonomous Policy

Install Policy Actions

Search for IP, object, action, ...

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	20K		* Any	* Any	* Any	NBT UDP port1900	Drop	None
2	29K		* Any	* Any	* Any	dns	Accept	None
3	72K	Pass all	* Any	* Any	* Any	* Any	Accept	Log

Standard +

Access Control

Policy

NAT

Threat Prevention

Custom Policy

Autonomous Policy

Exceptions

HTTPS Inspection

Policy

The Policy will be enforced only on gateways with HTTPS Inspection enabled. Don't show this message

Search for IP, object, action, ...

No.	Name	Source	Destination	Services	Category/Custom...	Action	Track	Blade
1	Predefined Rule	* Any	Internet	HTTPS default ser...	* Any	Inspect	Log	* All

Gateways

- Trusted CAs
- HTTPS Validation**
- Server Certificates

Network Objects

- Check Point
- Nodes
- Interoperable Devices
- Networks
- Groups
- Address Ranges
- Dynamic Objects

HTTPS Validation

Fail Mode

Note: The below feature is available for R80.10 Gateways and above.

- In case of internal system error:
- Bypass all requests (Fail-open)
 - Block all requests (Fail-close)

HTTPS Site Categorization Mode

Note: The below feature is available for R80.10 Gateways and above.

- Background - requests are allowed until categorization is complete
- Hold - requests are blocked until categorization is complete

Server Validation

- Drop traffic from servers with:
- Untrusted server certificate
 - Revoked server certificate (validate CRL)
 - Expired server certificate

Track validation errors

Automatically retrieve intermediate CA certificates

Certificate Blacklisting

Drop traffic from servers using the following certificates:

Certificate Serial Number	Comment
39:2a:43:4f:0e:07:df:1f:8a:a3:05:de:34:e0:...	login.yahoo.com
04:7e:cb:e9:fc:a5:5f:7b:d0:9e:ae:36:e1:0c:...	mail.google.com
00:e9:02:8b:95:78:e4:15:dc:1a:71:0a:2b:88:...	login.skype.com
08:64	e-ilem.kktmerkezbankasi.org
00:d7:55:8f:da:f5:f1:10:5b:b2:13:28:2b:70:...	login.yahoo.com

Track dropped traffic:

Whitelisting

Bypass HTTPS inspection of traffic to well known software update services (list is dynamically updated)

Troubleshooting

Log connections of clients that have not installed the CA certificate

