STUDERUS
network technologies

15:10 Uhr, Track 6C

Firewall-Funktionen im Detail

Armand Blechner, IT- und Kurs-Leiter, Studerus AG

STUDERUS
network technologies

Agenda

Grundprinzip Firewall

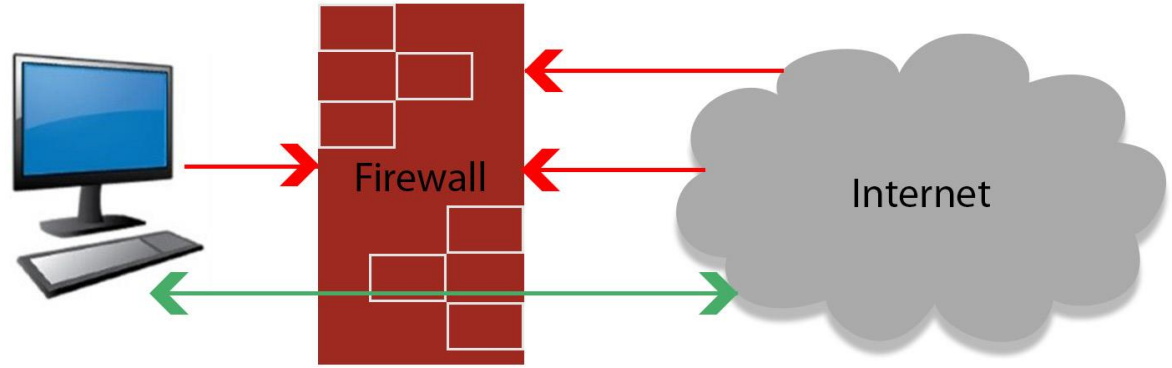
Allgemeine zusätzliche Funktionen (Dienste)

Übersicht Zyxel-Firewall / Zyxel-Dienste

Einsatz verfügbarer Mittel zum Schutz

Grundprinzip Firewall

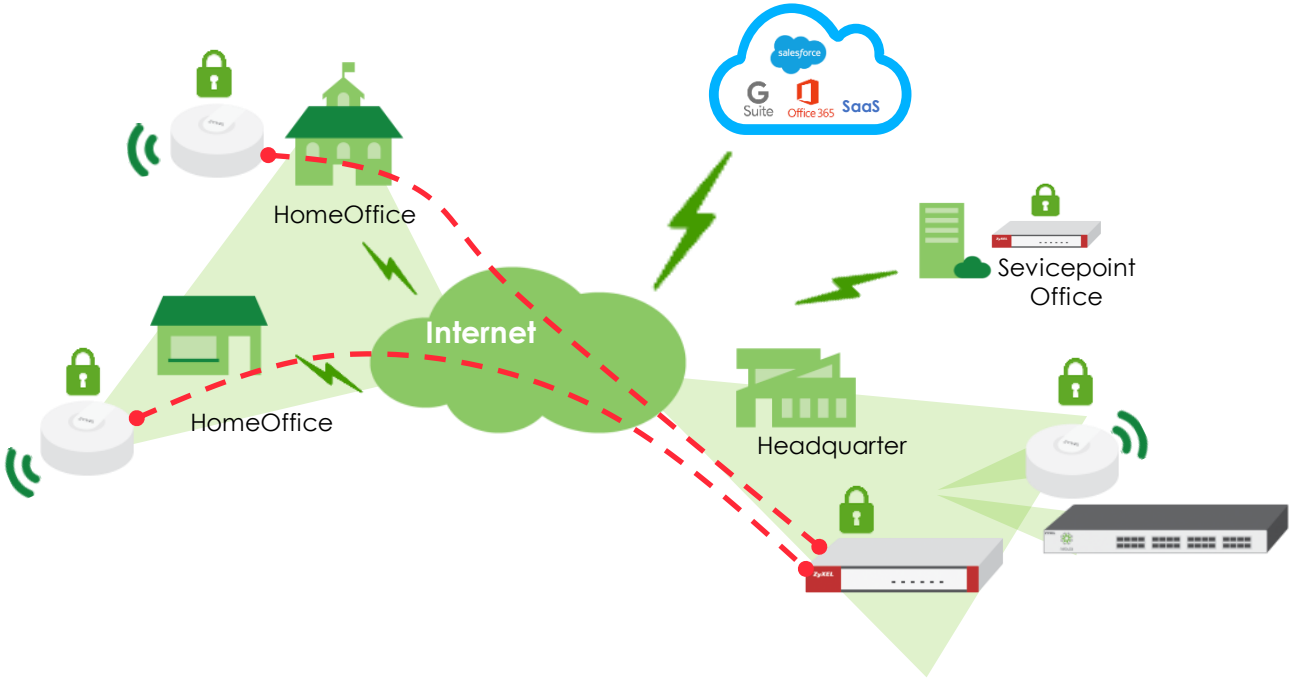
Grundschutz gegenüber andere Netzwerke (z.B. Internet)



unerlaubte Zugriffe werden von der Firewall blockiert
erlaubte Zugriffe werden zum Computer durchgelassen

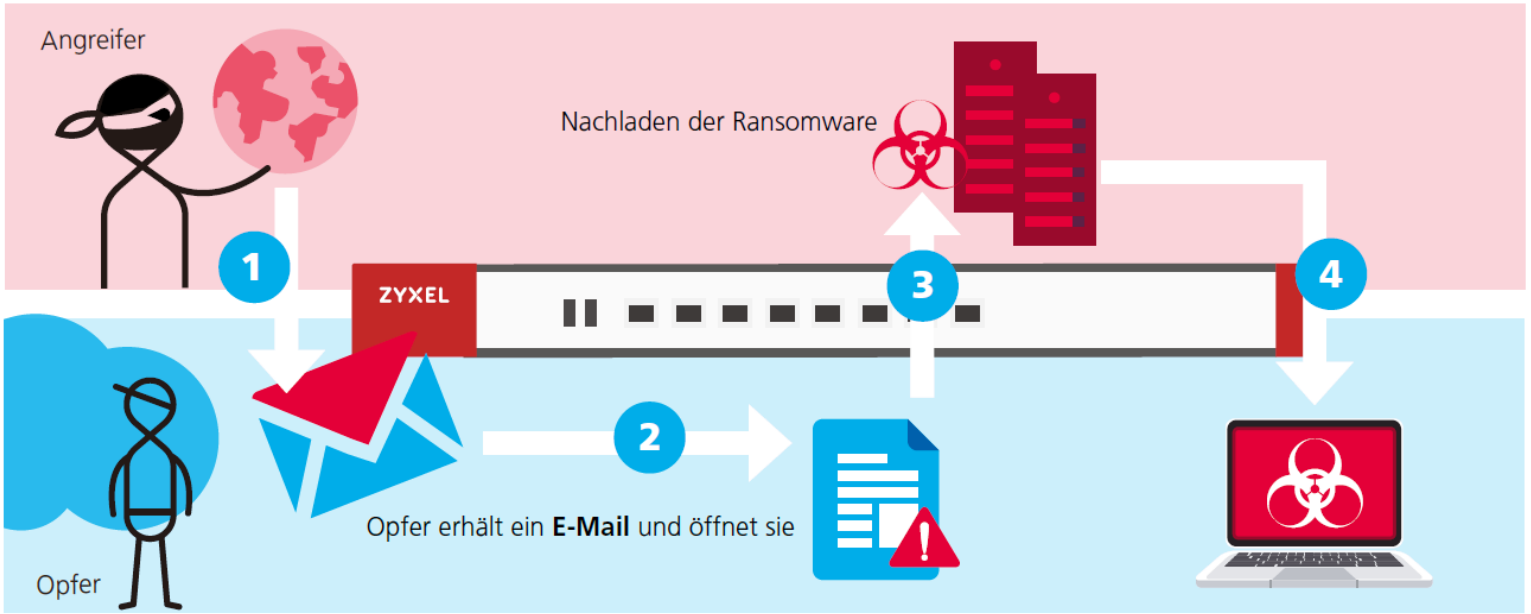
Beispielszenario

Gesicherte Kommunikation zwischen HQ und anderen Standorten, Nutzung von Cloud-Diensten



Beispielszenario Angriff

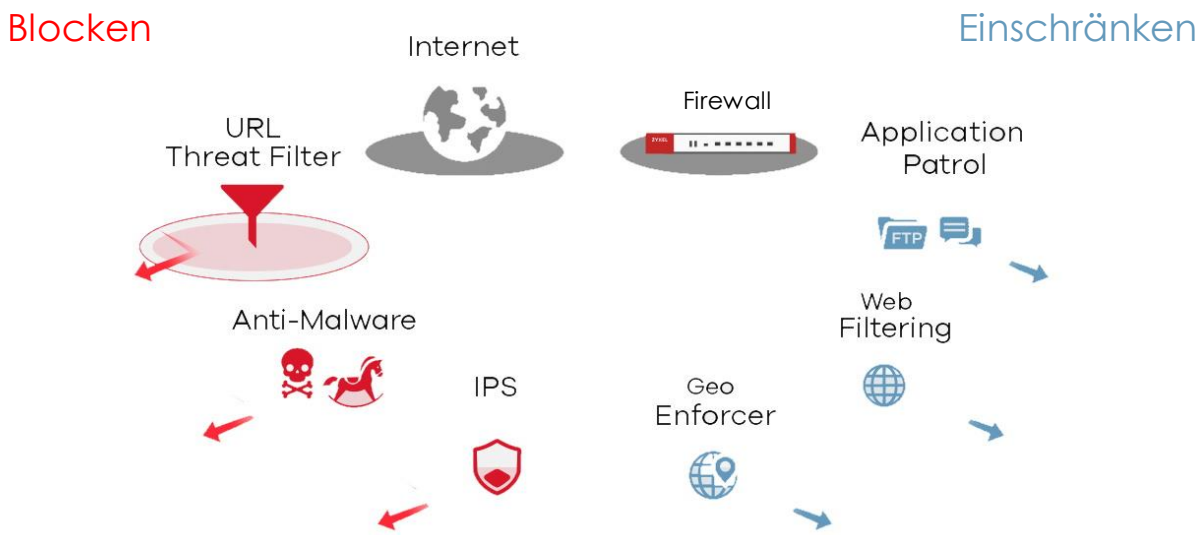
Beispiel Ablauf eines Ransomware-Angriffs



1. Opfer erhält ein E-Mail mit einem Link oder Attachment
2. Der Link oder das Attachment wird geöffnet
3. Ransomware wird von einer kompromittierten Website nachgeladen
4. Ransomware wird auf dem Rechner installiert und versucht sich im Netzwerk zu verbreiten

Allgemeine zusätzliche Funktionen

Erweiterter Schutz gegenüber andere Netzwerke (z.B. Internet)



Zyxel-Dienste

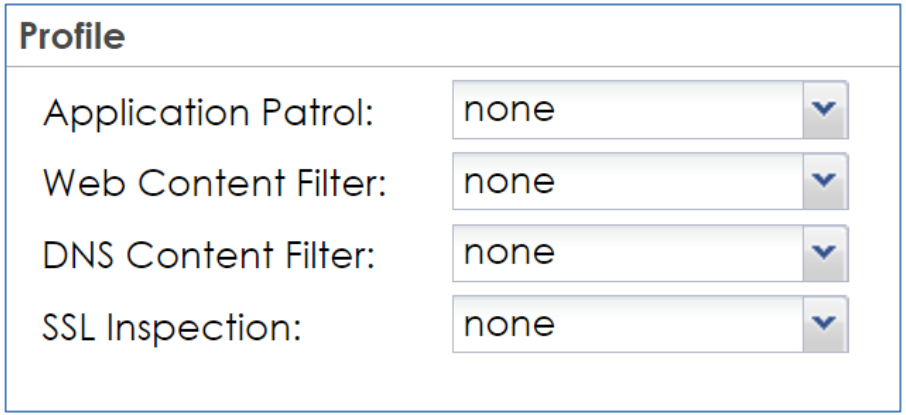
Erweiterter Schutz gegenüber anderen Netzwerken (z.B. Internet)

- Anomaly Prevention
- Reputation Filter
- Intrusion Prevention
- Anti-Malware
- Sandboxing
- Email-Security

Zyxel-Dienste

Erweiterter Schutz gegenüber anderen Netzwerken (z.B. Internet)

- Application Patrol
- DNS/Web Content Filter
- SSL-Inspection
- Geo Enforcer/GeoIP
- Device Insight



- Analysetool SecuReporter

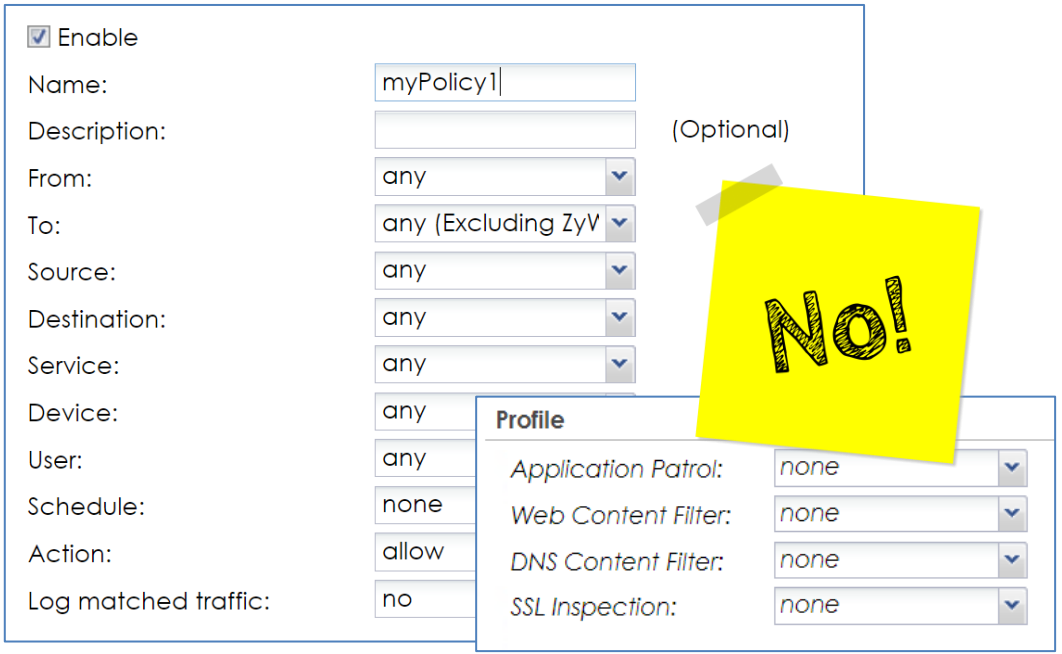
Einsatz verfügbarer Mittel

STUDERUS
network technologies

Zyxel-Firewalls verfügbare Mittel

Regelwerk, nur nötigen Traffic

Quelle/Ziel (IP)
Protokoll
Device
Zeitfenster
erlauben/verweigern
Log aktiv
Sicherheitsprofile



Konkrete Einstellungen

Quelle / Ziel

Zonen (From/To)

Source

Destination

From	To	IPv4 Source	IPv4 Desti...	Service
WAN	LAN1	any	pbx_IP	pbx_ports
WAN	LAN2	any	nerves	TCP8080
WAN	LAN2	any	nerves	myWeb
WAN	LAN2	any	nerves	myBilling
WAN	LAN2	any	monitori...	Monitori...

8		LAN2_Outgoing	LAN2	WAN	LAN2_SUBNET

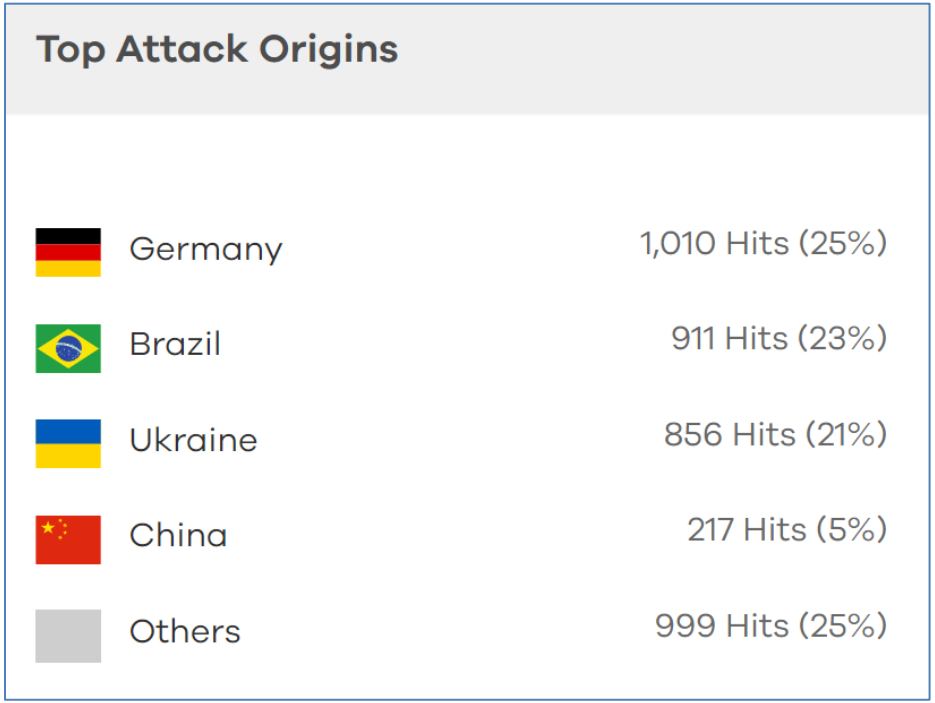
Konkrete Einstellungen

Geo Enforcer

SecuReporter hilft:

Einzelne Geo-Bereiche erlauben

Restliche Geo-Bereiche droppen



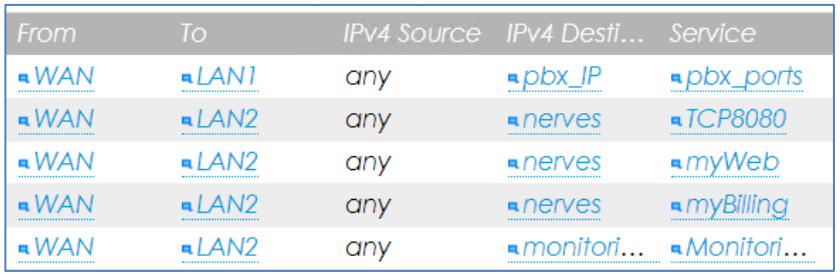
Konkrete Einstellungen

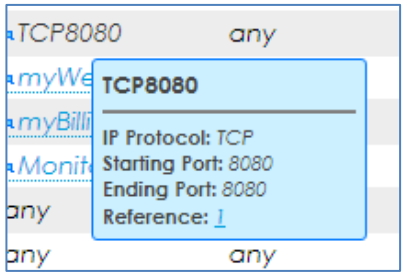
Protokoll

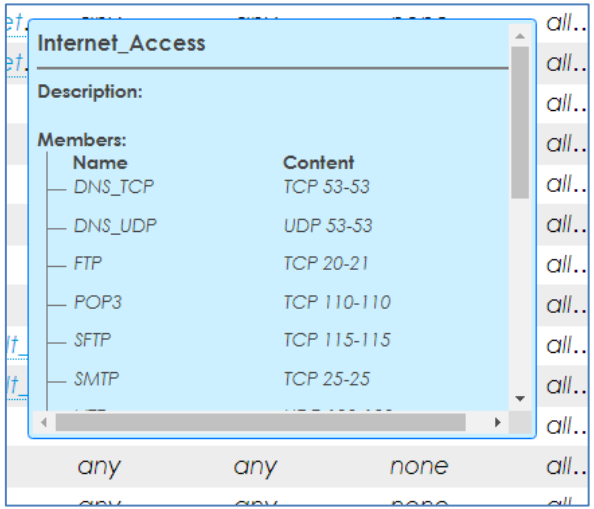
Einzelne Ports

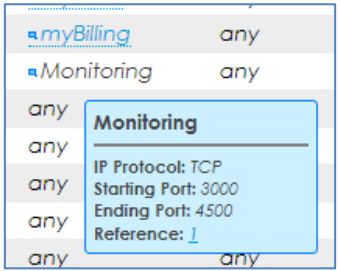
Port-Bereiche

Gruppen







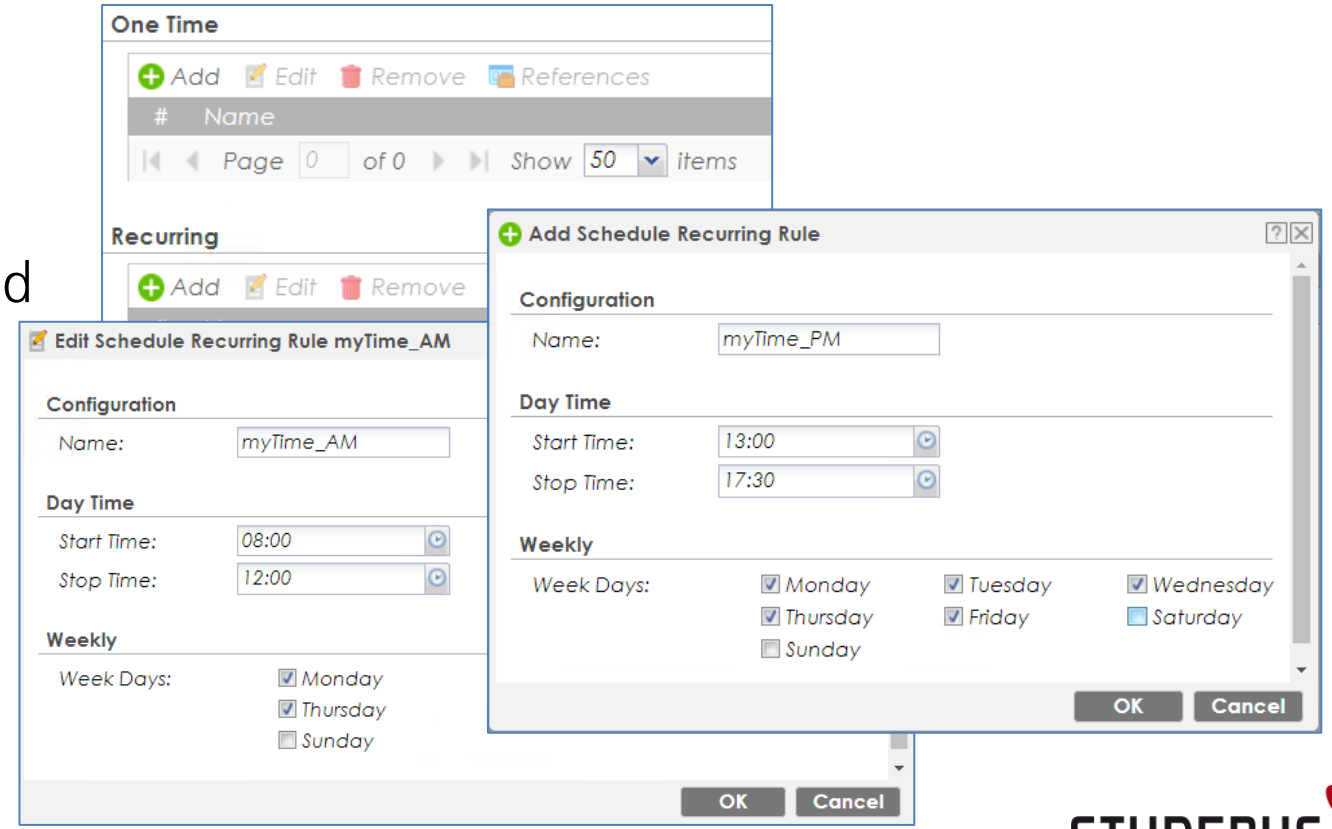


Konkrete Einstellungen

Zeitfenster

einmalig

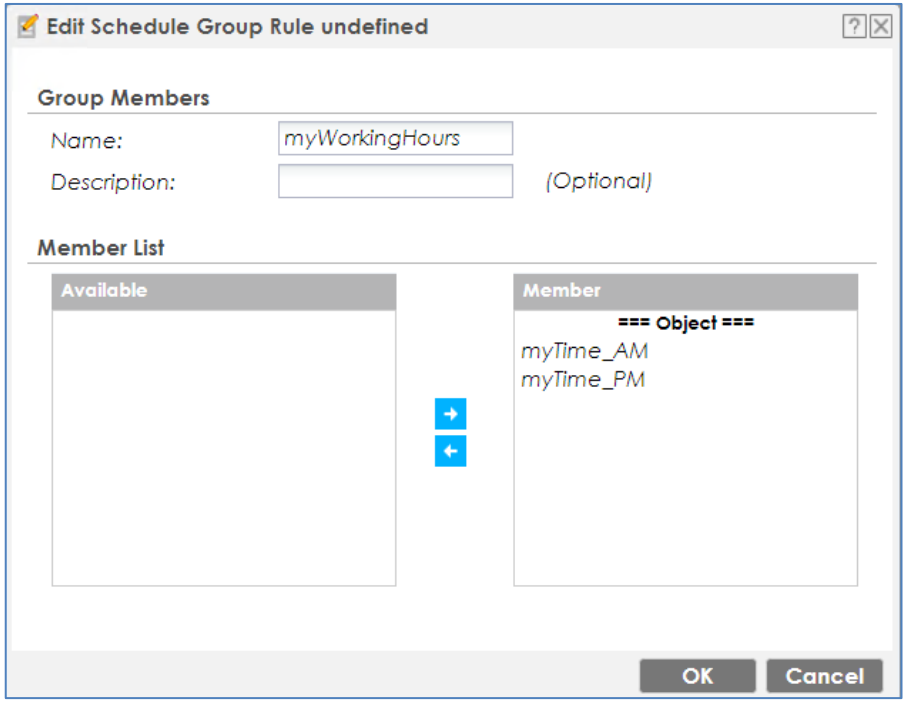
wiederkehrend



Konkrete Einstellungen

Zeitfenster

gruppiert



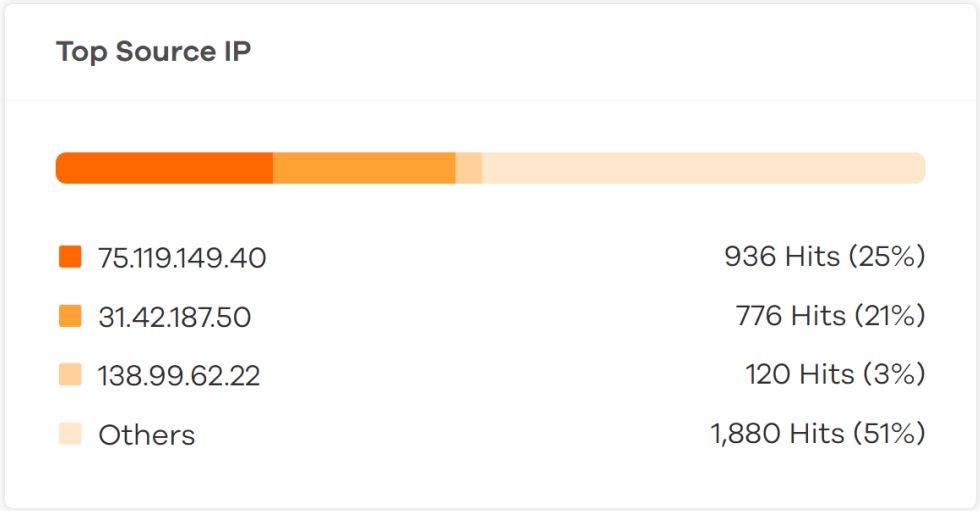
Zyxel-Firewalls verfügbare Mittel

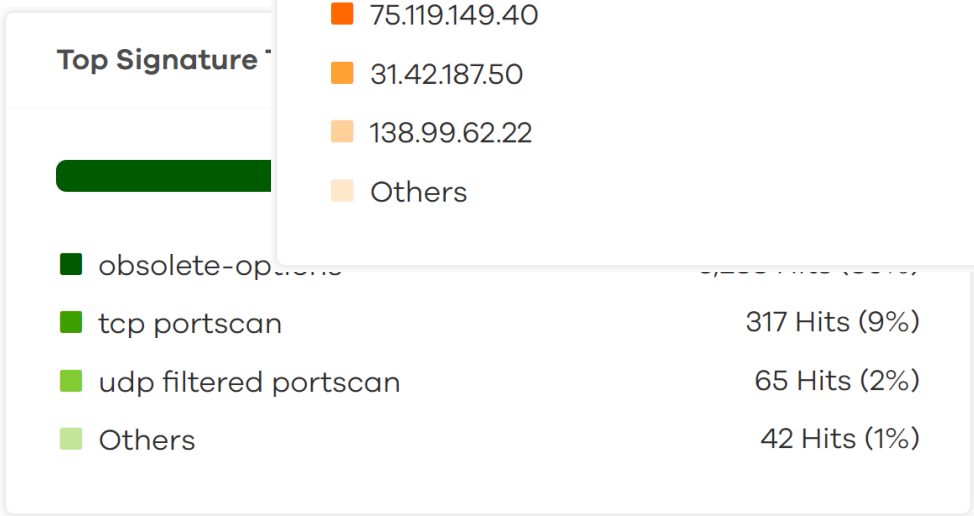
Anomaly Prevention

SecuReporter hilft:

Attacken erkennen

IPs droppen





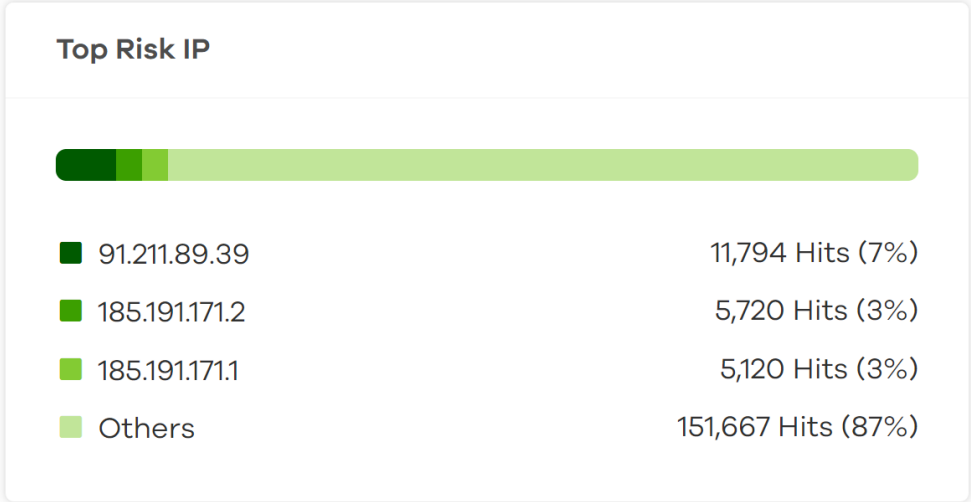
Zyxel-Firewalls verfügbare Mittel

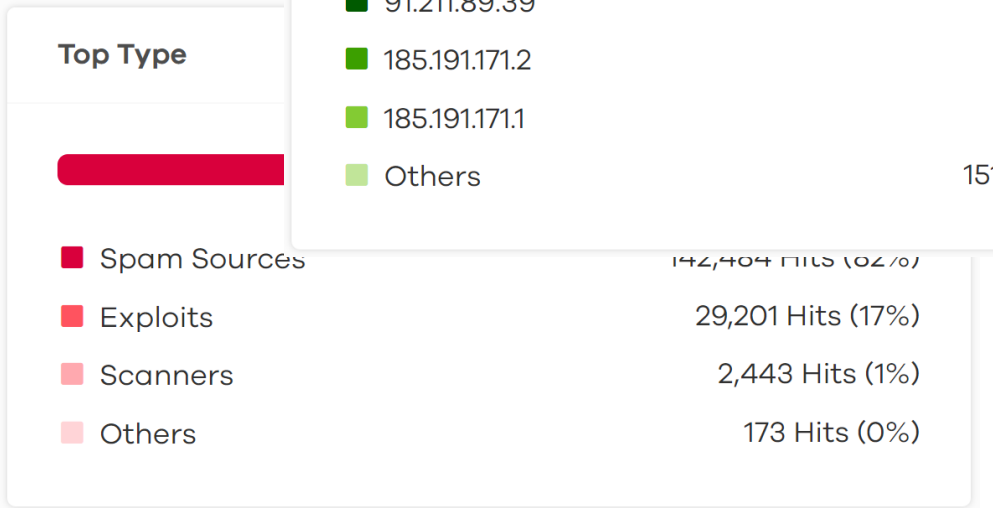
Reputation Filter

SecuReporter hilft:

Attacken erkennen

IPs droppen





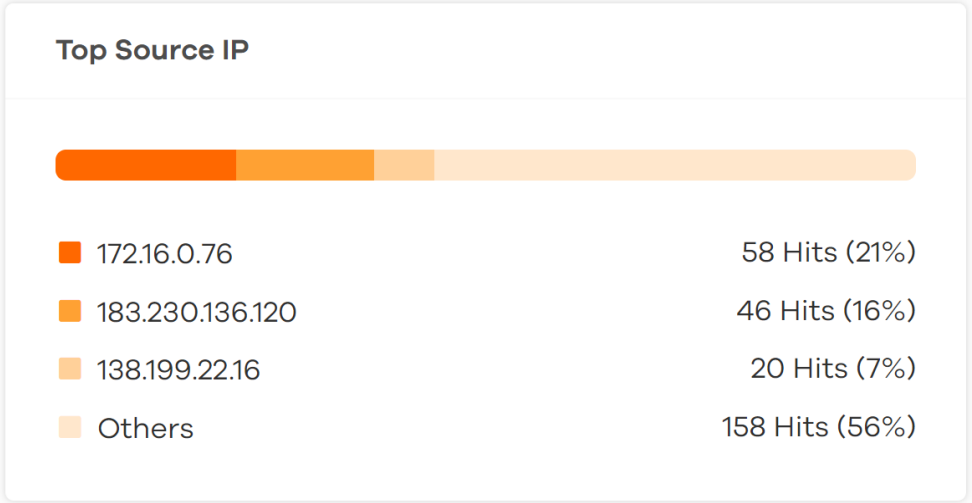
Zyxel-Firewalls verfügbare Mittel

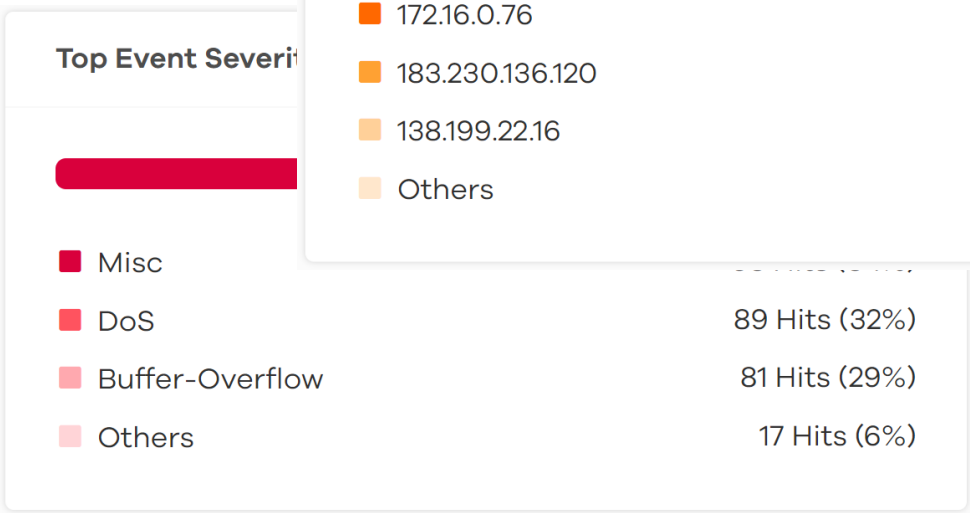
Intrusion Prevention

SecuReporter hilft:

Attacken erkennen

IPs droppen

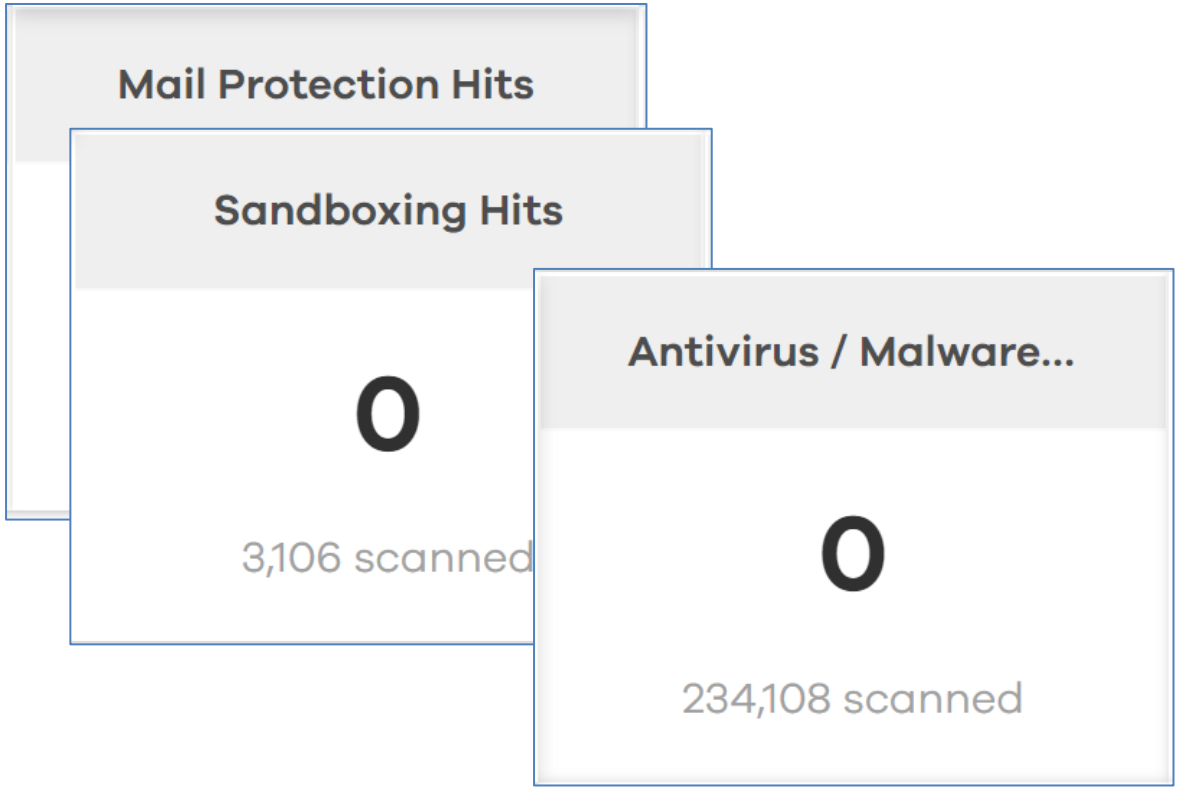




Zyxel-Firewalls verfügbare Mittel

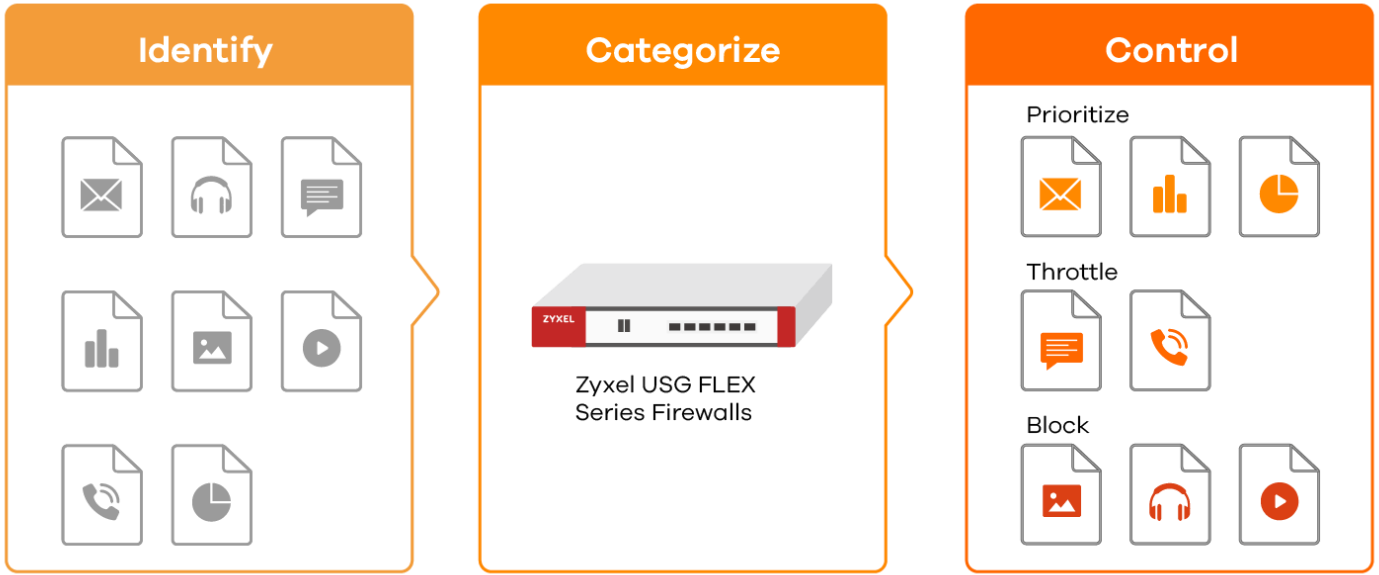
- Anti Malware
- Sandboxing
- Mail Protection

SecuReporter hilft:



Zyxel-Firewalls verfügbare Mittel

App Patrol



Beispiele App Patrol

Erweiterter Schutz gegenüber andere Netzwerke (z.B. Internet)

Statistics

#	Application
1	HyperText Transfer Protocol Secure
2	VMWare Horizon
3	Microsoft teams
4	Microsoft Outlook (Office 365)
5	Windows Update
6	Bingbot
7	GoogleBot
8	Youtube.com
9	Adobe Creative Cloud
10	Microsoft Azure (previously Window…
11	Tabular Data Stream
12	Microsoft Office 365
13	Akamai Technologies CDN	18940531
14	Remote Desktop Protocol (Window…	16556734
15	File Transfer Protocol Data	15313084
16	Real Time Protocol	
17	IPsec (AH and ESP)	
18	Amazon Web Services/Cloudfron	
19	Microsoft OneDrive	
20	Vmware Horizon View (PCoIP prot	
21	Microsoft SharePoint Online (Offic	
22	Simple Mail Transfer Protocol	
23	Microsoft	
24	CloudFlare CDN	
25	Windows Management Instrumen	
26	Google APIs	
27	Micosoft Edge	
28	Netflix.com	
29	Adobe	
30	LinkedIn	
31	Server Message Block (Windows F	
32	Google Ads	
33	Chrome Update	
34	Google Search	4073518
35	HyperText Transfer Protocol version 2	3327094
36	GoToMeeting Online Meeting	3306755
37	Kaspersky Update	3189092
38	Zoom	3118093
39	Google Documents (aka Google D…	2433089
40	AppNexus	2342881
41	Facebook	2163899
42	Bing.com (formerly MSN Search)	2101263
43	HyperText Transfer Protocol	2070686
44	Digicert	2021682
45	VMWare	2004787
46	Zendesk	1913389
47	Windows Marketplace	1908550
48	Google Play Store	1894743
49	Google GStatic	1887234
50	HubSpot	1849642

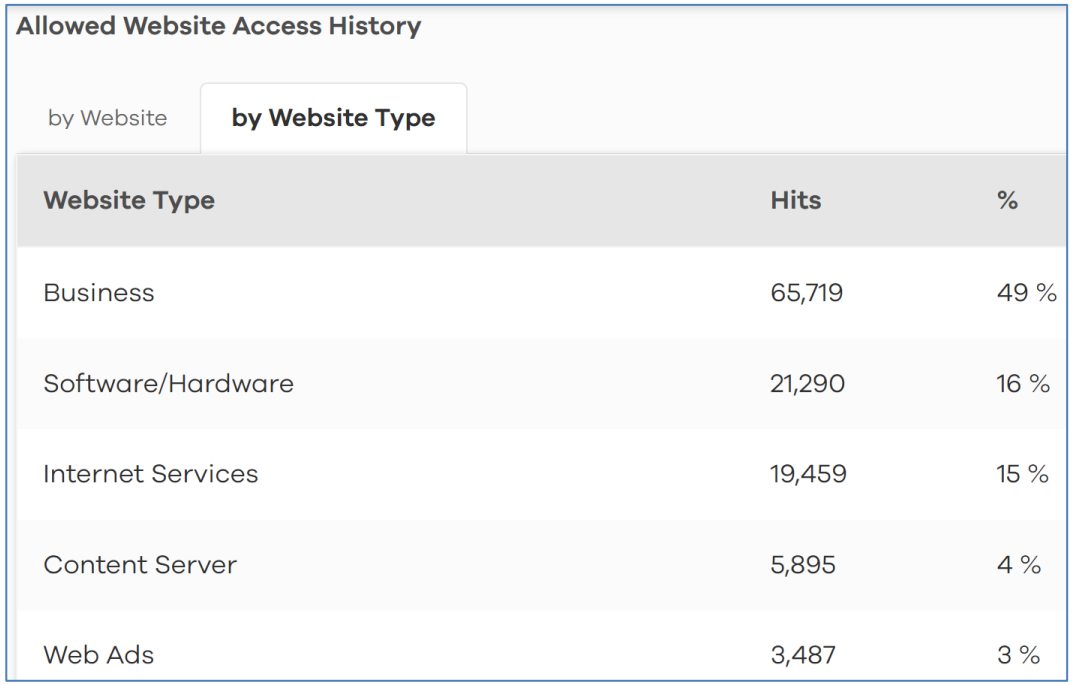
Zyxel-Firewalls verfügbare Mittel

Content Filter

SecuReporter hilft:

Kategorien identifizieren

Kategorien einschränken



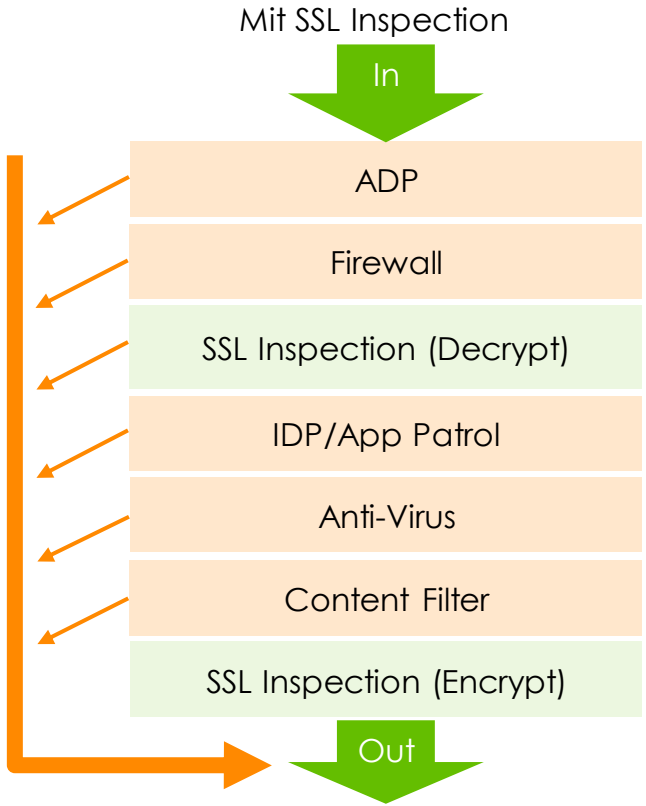
Allowed Website Access History

by Website | **by Website Type**

Website Type	Hits	%
Business	65,719	49 %
Software/Hardware	21,290	16 %
Internet Services	19,459	15 %
Content Server	5,895	4 %
Web Ads	3,487	3 %

Zyxel-Firewalls verfügbare Mittel

SSL-Inspection



Zyxel-Firewalls verfügbare Mittel

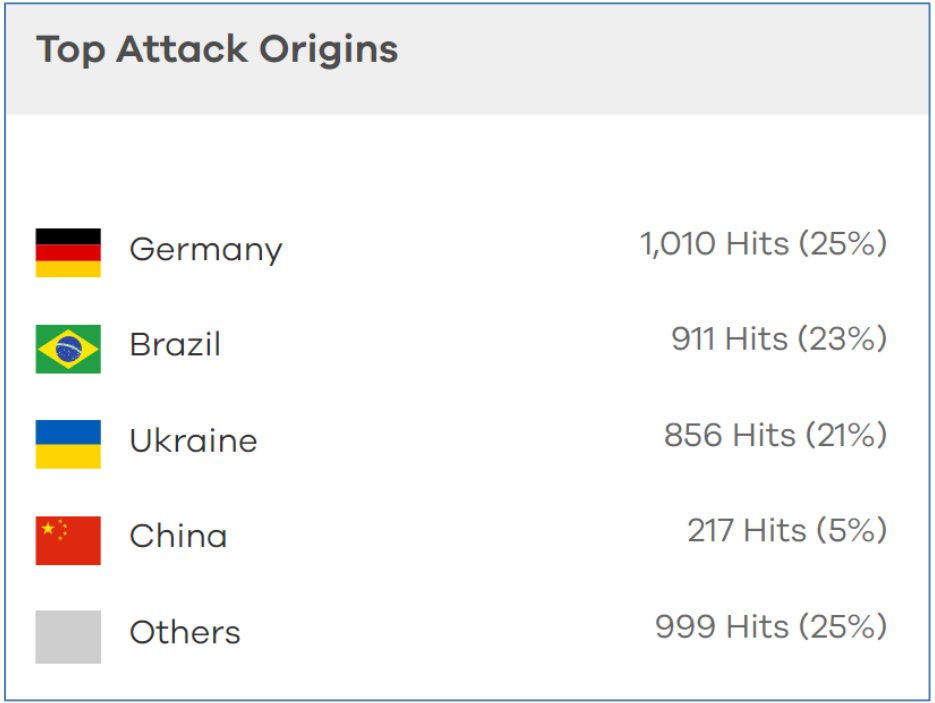
Geo Enforcer

SecuReporter hilft:

Attacken erkennen

Einzelne Geo-Bereiche erlauben

Restliche Geo-Bereiche droppen

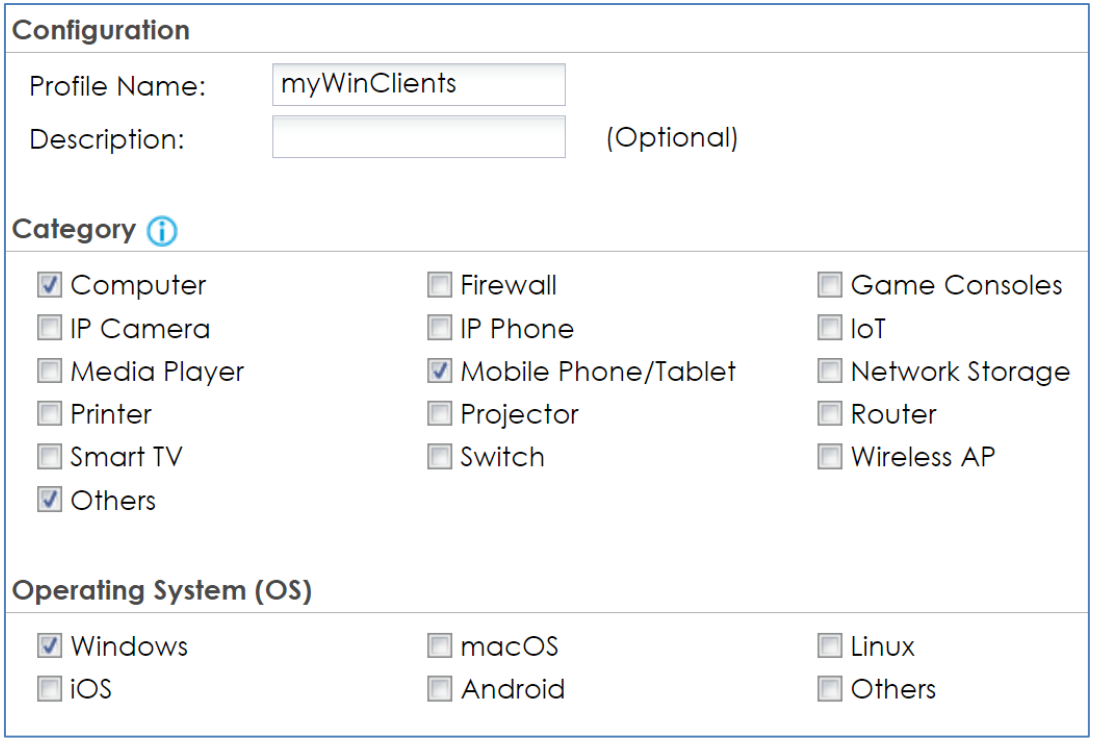


Zyxel-Firewalls verfügbare Mittel

Device Insight

Geräte-Kategorie

Policy nach OS

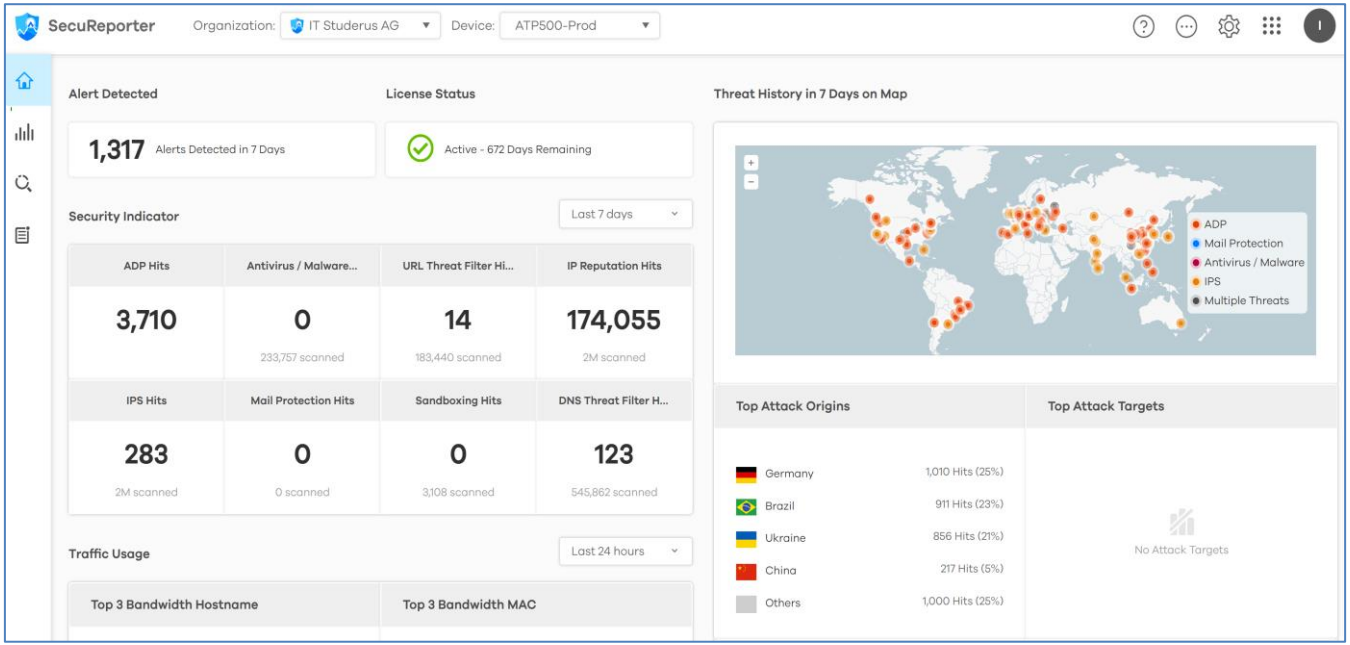


Zyxel-Firewalls verfügbare Mittel

SecuReporter

Analyse

Reporting



Zywall Series Highlights

2022

STUDERUS
network technologies

STUDERUS
network technologies