

A black and white photograph of a man in a dark suit, seen from behind, gesturing with his right hand towards a large, blurred audience seated in a conference hall. The background is out of focus, showing rows of people and stage lights.

TE
FO22

15:10 Uhr, Track 6C

Firewall-Funktionen im Detail

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

Agenda

Grundprinzip Firewall

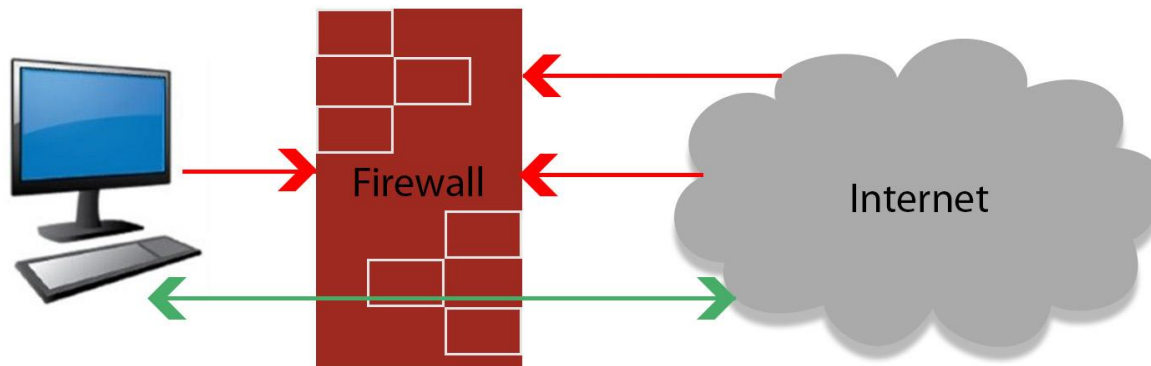
Allgemeine zusätzliche Funktionen (Dienste)

Übersicht Zykel-Firewall / Zykel-Dienste

Einsatz verfügbarer Mittel zum Schutz

Grundprinzip Firewall

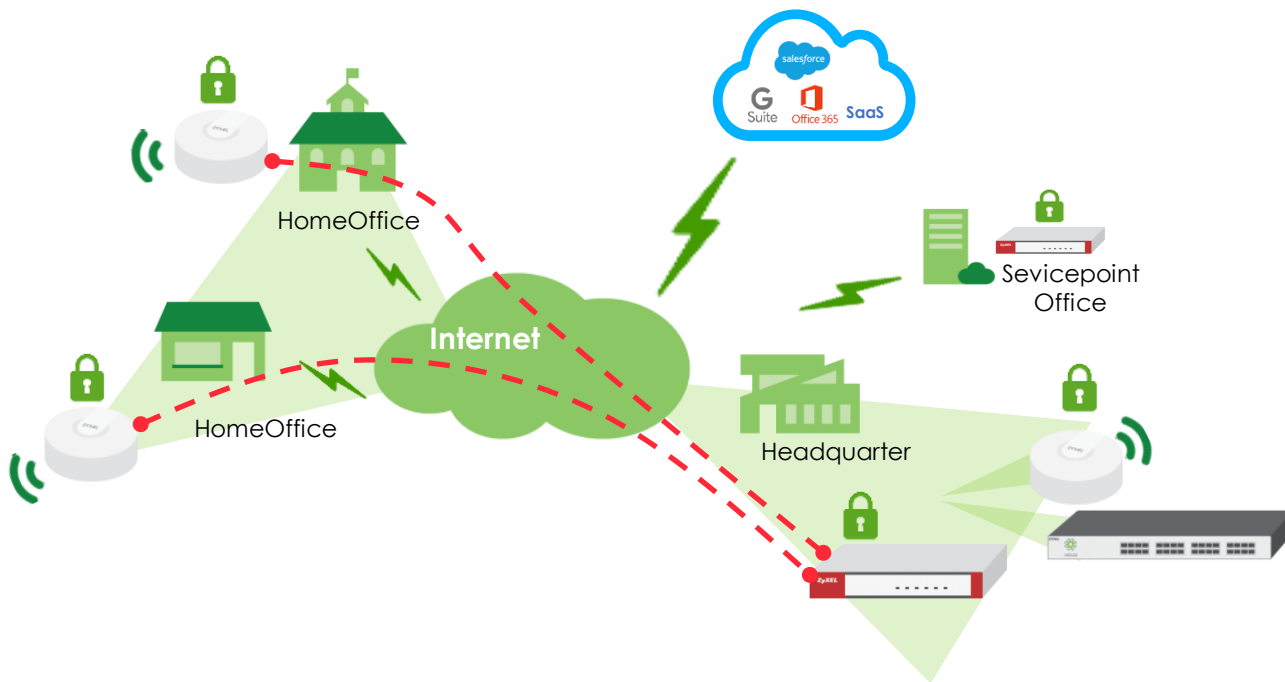
Grundschutz gegenüber andere Netzwerke (z.B. Internet)



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

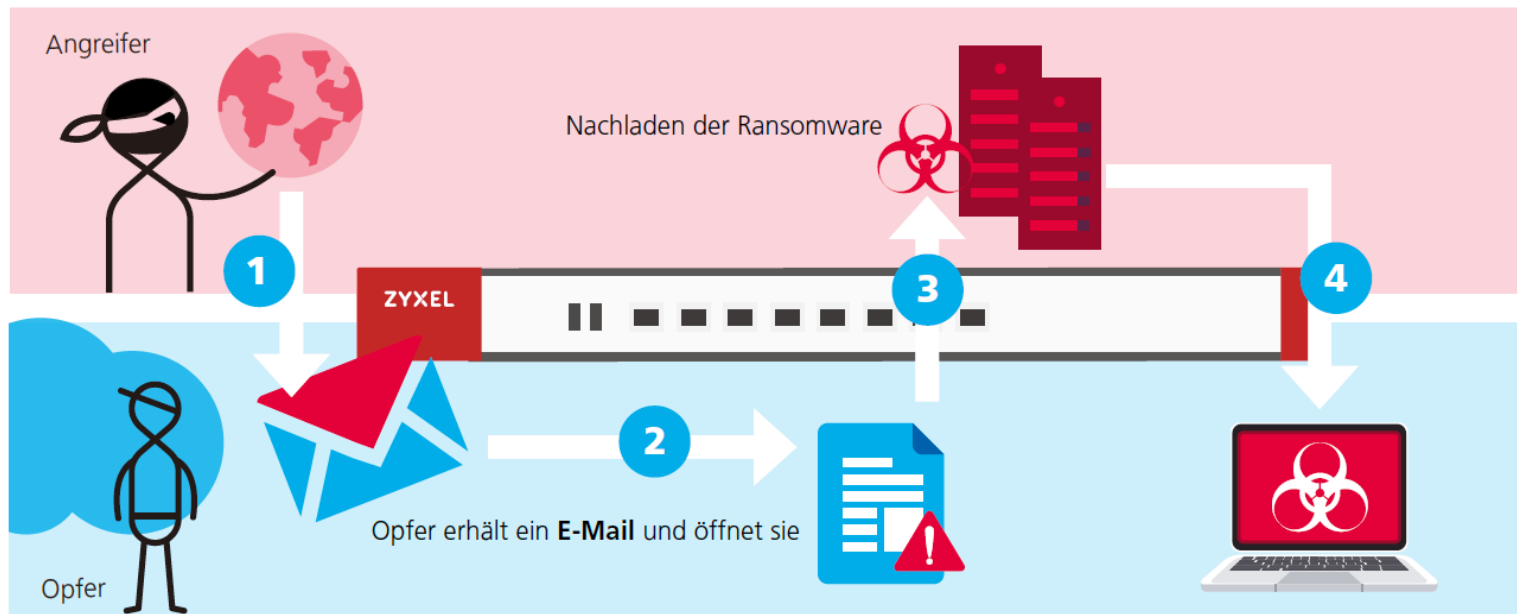
Beispielszenario

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



Beispielszenario Angriff

Beispiel Ablauf eines Ransomware-Angriffs



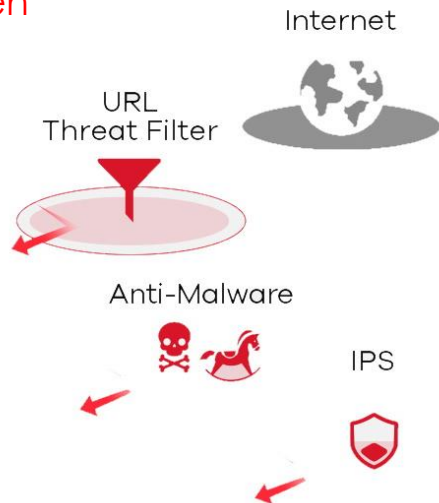
- 1 Opfer erhält ein E-Mail mit einem Link oder Attachment
- 2 Der Link oder das Attachment wird geöffnet

- 3 Ransomware wird von einer kompromittierten Website nachgeladen
- 4 Ransomware wird auf dem Rechner installiert und versucht sich im Netzwerk zu verbreiten

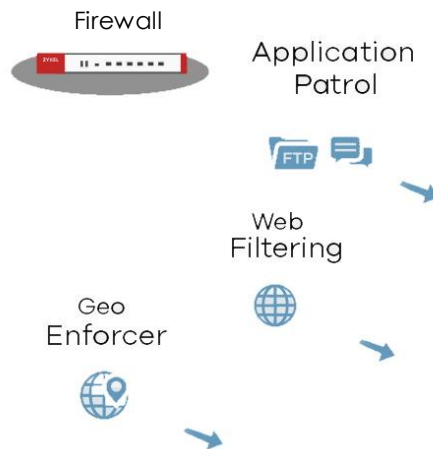
Allgemeine zusätzliche Funktionen

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

Blocken



Einschränken



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

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

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

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

Profile	
Application Patrol:	none ▼
Web Content Filter:	none ▼
DNS Content Filter:	none ▼
SSL Inspection:	none ▼



Einsatz verfügbarer Mittel

Zykel-Firewalls verfügbare Mittel

Regelwerk, nur nötigen Traffic

Quelle/Ziel (IP)

Protokoll

Device

Zeitfenster

erlauben/verweigern

Log aktiv

Sicherheitsprofile

☒ Enable

Name:

Description: (Optional)

From: ▼

To: ▼

Source: ▼

Destination: ▼

Service: ▼

Device:

User:

Schedule:

Action:

Log matched traffic:

Profile

Application Patrol: ▼

Web Content Filter: ▼

DNS Content Filter: ▼

SSL Inspection: ▼

No!

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 dropen

Top Attack Origins

	Germany	1,010 Hits (25%)
	Brazil	911 Hits (23%)
	Ukraine	856 Hits (21%)
	China	217 Hits (5%)
	Others	999 Hits (25%)

Konkrete Einstellungen

Protokoll

Einzelne Ports

Port-Bereiche

Gruppen

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...

TCP8080	any
myWe	TCP8080
myBilli	TCP8080
Moniti	TCP8080
any	any
any	any

TCP8080
IP Protocol: TCP
Starting Port: 8080
Ending Port: 8080
Reference: [1](#)

Internet_Access	
Description:	
Members:	
Name	Content
DNS_TCP	TCP 53-53
DNS_UDP	UDP 53-53
FTP	TCP 20-21
POP3	TCP 110-110
SFTP	TCP 115-115
SMTP	TCP 25-25

myBilling	any
Monitoring	any
any	any
any	any
any	any
any	any
any	any

Monitoring
IP Protocol: TCP
Starting Port: 3000
Ending Port: 4500
Reference: [1](#)

Konkrete Einstellungen

Zeitfenster

einmalig

wiederkehrend

The image displays a software interface for configuring time windows. It features two main sections: 'One Time' and 'Recurring'. The 'One Time' section has a table with columns '#', 'Name', and a toolbar with '+ Add', 'Edit', 'Remove', and 'References'. The 'Recurring' section also has a toolbar with '+ Add', 'Edit', and 'Remove'. Two overlapping dialog boxes are shown. The 'Edit Schedule Recurring Rule myTime_AM' dialog box has a 'Configuration' section with a 'Name' field set to 'myTime_AM'. Below this is a 'Day Time' section with 'Start Time' (08:00) and 'Stop Time' (12:00) fields. At the bottom is a 'Weekly' section with 'Week Days' checkboxes for Monday, Thursday, and Sunday. The 'Add Schedule Recurring Rule' dialog box has a 'Configuration' section with a 'Name' field set to 'myTime_PM'. Below this is a 'Day Time' section with 'Start Time' (13:00) and 'Stop Time' (17:30) fields. At the bottom is a 'Weekly' section with 'Week Days' checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Both dialog boxes have 'OK' and 'Cancel' buttons at the bottom.

One Time

+ Add Edit Remove References

#	Name
---	------

Page 0 of 0 Show 50 items

Recurring

+ Add Edit Remove

Edit Schedule Recurring Rule myTime_AM

Configuration

Name: myTime_AM

Day Time

Start Time: 08:00

Stop Time: 12:00

Weekly

Week Days: ☒ Monday ☒ Thursday ☐ Sunday

Add Schedule Recurring Rule

Configuration

Name: myTime_PM

Day Time

Start Time: 13:00

Stop Time: 17:30

Weekly

Week Days: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday ☐ Sunday

OK Cancel

Konkrete Einstellungen

Zeitfenster

gruppiert

Edit Schedule Group Rule undefined

Group Members

Name:

Description: (Optional)

Member List

Available	Member
	=== Object === myTime_AM myTime_PM

OK Cancel

Zyxel-Firewalls verfügbare Mittel

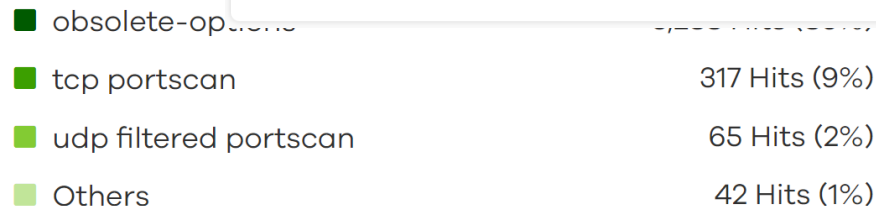
Anomaly Prevention

SecuReporter hilft:
Attacken erkennen
IPs dropen

Top Source IP



Top Signature



Zyxel-Firewalls verfügbare Mittel

Reputation Filter

SecuReporter hilft:

Attacken erkennen

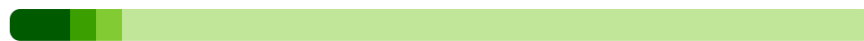
IPs dropen

Top Type



Spam Sources	142,404 Hits (62%)
Exploits	29,201 Hits (17%)
Scanners	2,443 Hits (1%)
Others	173 Hits (0%)

Top Risk IP



91.211.89.39	11,794 Hits (7%)
185.191.171.2	5,720 Hits (3%)
185.191.171.1	5,120 Hits (3%)
Others	151,667 Hits (87%)

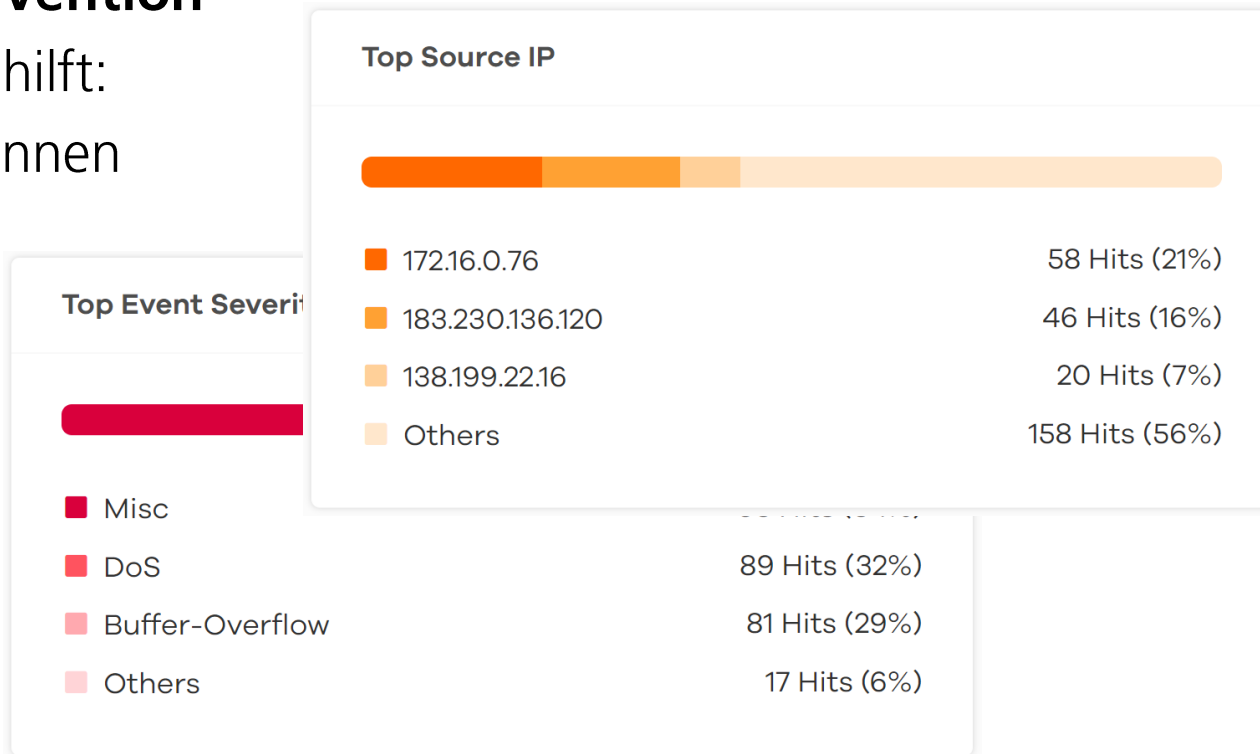
Zyxel-Firewalls verfügbare Mittel

Intrusion Prevention

SecuReporter hilft:

Attacken erkennen

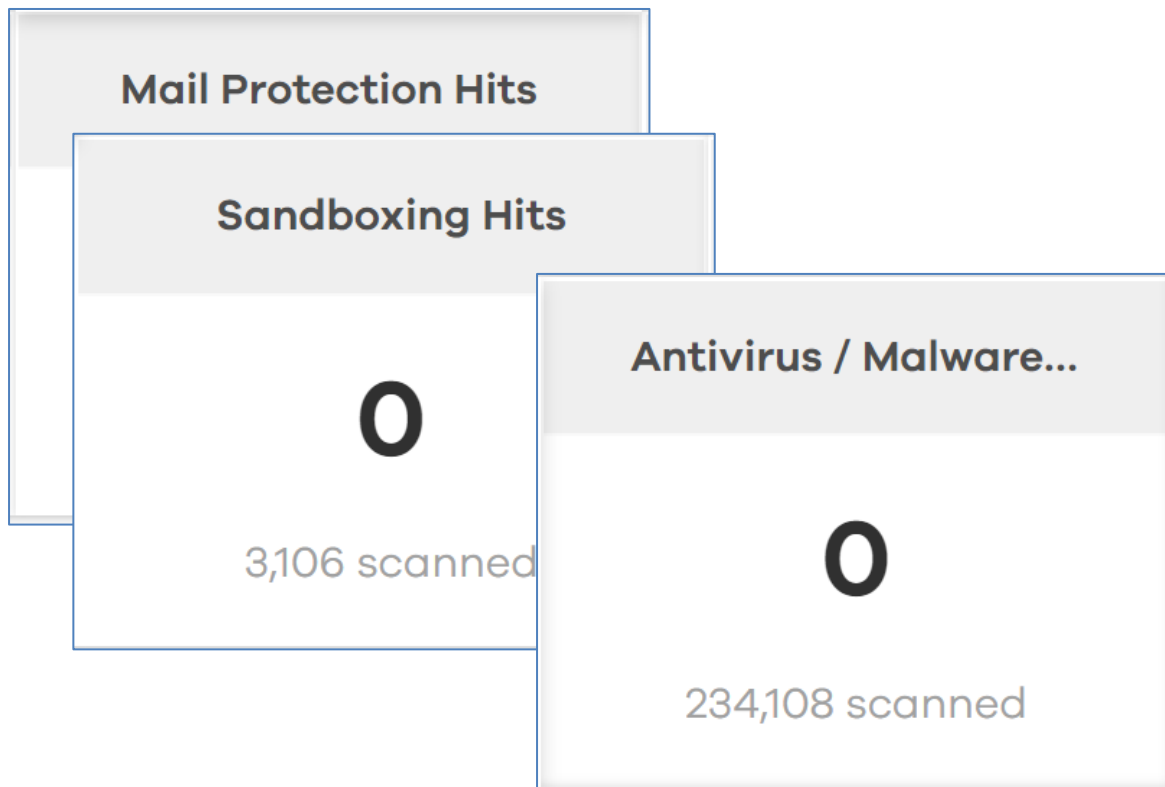
IPs dropen



Zyxel-Firewalls verfügbare Mittel

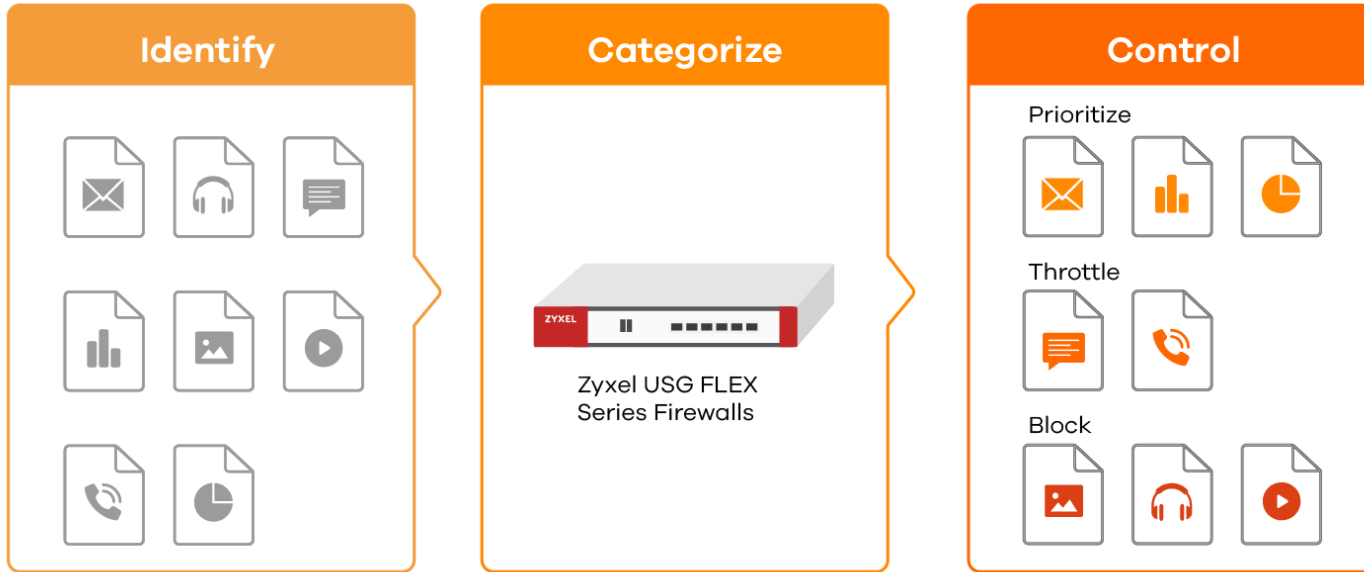
- Anti Malware
- Sandboxing
- Mail Protection

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	13	Akamai Technologies CDN 18940531
2	VMWare Horizon	14	Remote Desktop Protocol (Window... 16556734
3	Microsoft teams	15	File Transfer Protocol Data 15312084
4	Microsoft Outlook (Office 365)	16	Real Time Protocol
5	Windows Update	17	IPsec (AH and ESP)
6	Bingbot	18	Amazon Web Services/Cloudfront
7	GoogleBot	19	Microsoft OneDrive
8	Youtube.com	20	Vmware Horizon View (PCoIP prot
9	Adobe Creative Cloud	21	Microsoft SharePoint Online (Offic
10	Microsoft Azure (previously Window...	22	Simple Mail Transfer Protocol
11	Tabular Data Stream	23	Microsoft
12	Microsoft Office 365	24	CloudFlare CDN
		25	Windows Management Instrumen
		26	Google APIs
		27	Microsoft 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:

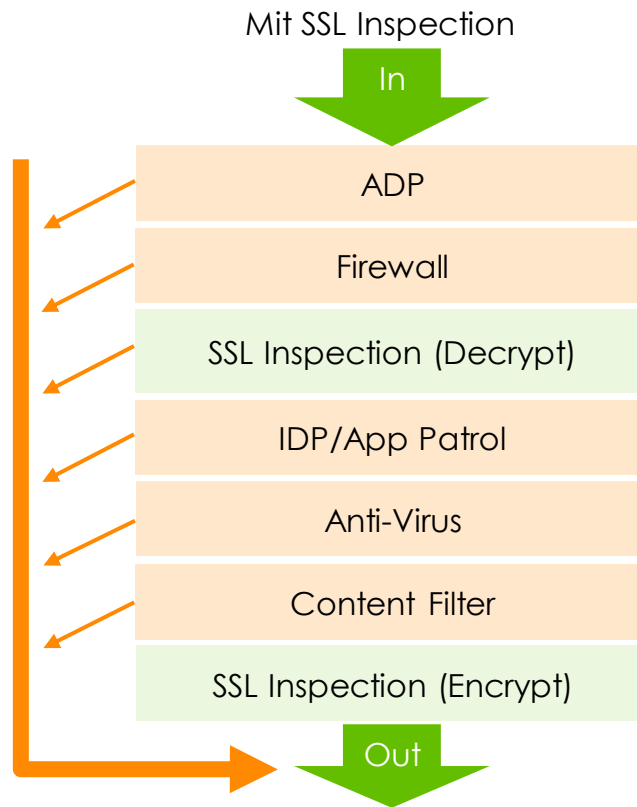
Kategorien identifizieren

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 dropen

Top Attack Origins

	Germany	1,010 Hits (25%)
	Brazil	911 Hits (23%)
	Ukraine	856 Hits (21%)
	China	217 Hits (5%)
	Others	999 Hits (25%)

Zyxel-Firewalls verfügbare Mittel

Device Insight

Geräte-Kategorie

Policy nach OS

Configuration

Profile Name:

Description: (Optional)

Category ⓘ

☒ Computer	☐ Firewall	☐ Game Consoles
☐ IP Camera	☐ IP Phone	☐ IoT
☐ Media Player	☒ Mobile Phone/Tablet	☐ Network Storage
☐ Printer	☐ Projector	☐ Router
☐ Smart TV	☐ Switch	☐ Wireless AP
☒ Others		

Operating System (OS)

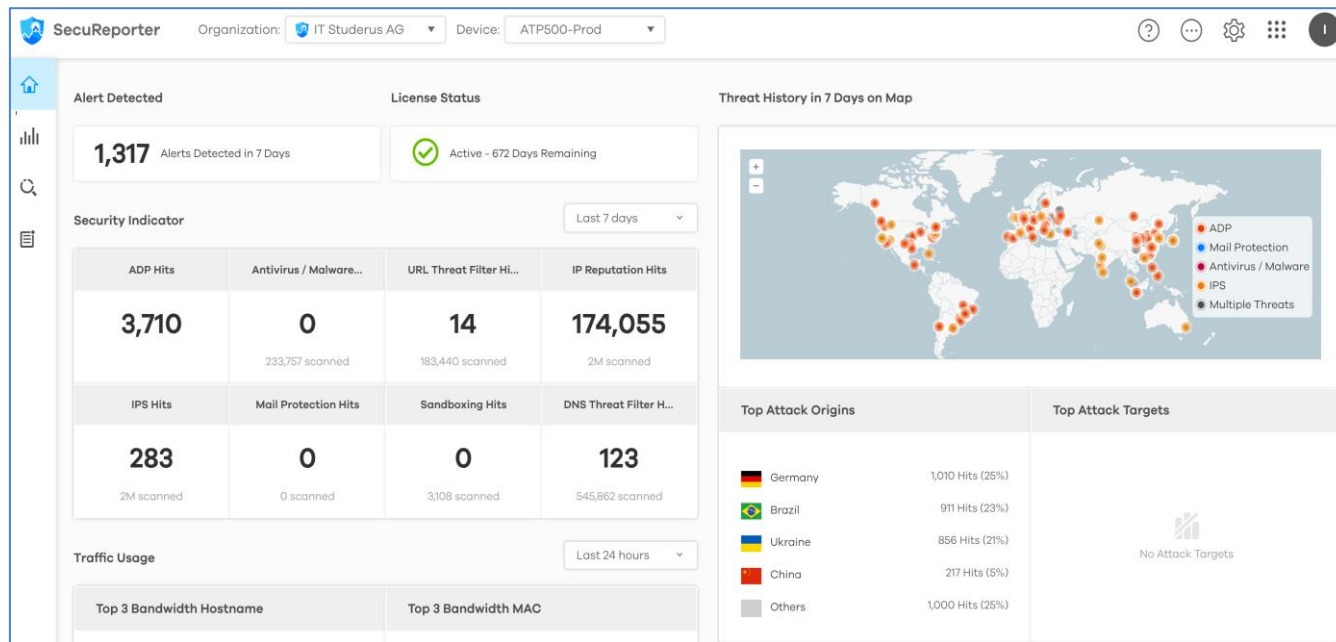
☒ Windows	☐ macOS	☐ Linux
☐ iOS	☐ Android	☐ Others

Zyxel-Firewalls verfügbare Mittel

SecuReporter

Analyse

Reporting





Zywall Series Highlights

2022

A black and white photograph of a man in a dark suit, seen from behind, gesturing with his right hand towards a large, blurred audience seated in a conference hall. The background is out of focus, showing rows of people and stage lights.

TE
FO22