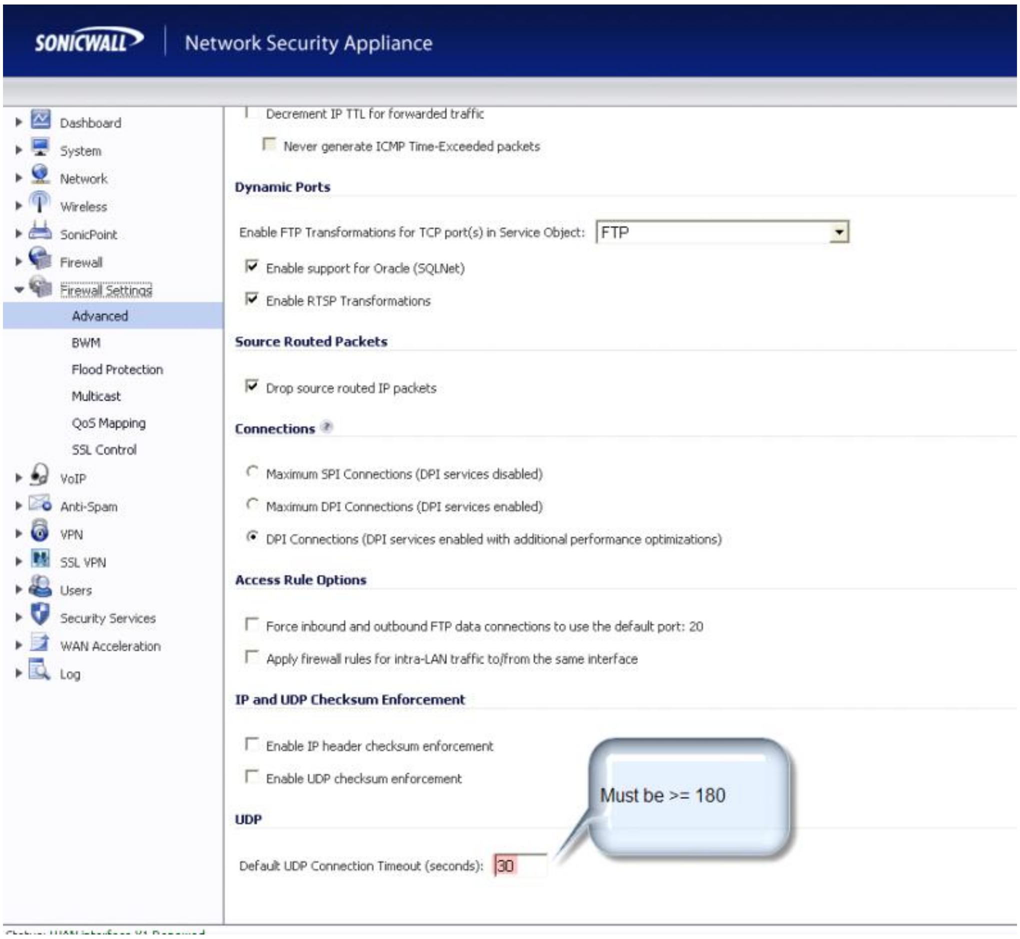
Sonicwall

Dienstag, 13. September 2011
11:14

Erst ab Softwarestand 5.7 läuft Bcon sauber



□ Decrement IP TTL for forwarded traffic

□ Never generate ICMP Time-Exceeded packets

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object: FTP

☑ Enable support for Oracle (SQLNet)

☑ Enable RTSP Transformations

Source Routed Packets

☑ Drop source routed IP packets

Connections

○ Maximum SPI Connections (DPI services disabled)

○ Maximum DPI Connections (DPI services enabled)

● DPI Connections (DPI services enabled with additional performance optimizations)

Access Rule Options

□ Force inbound and outbound FTP data connections to use the default port: 20

□ Apply firewall rules for intra-LAN traffic to/from the same interface

IP and UDP Checksum Enforcement

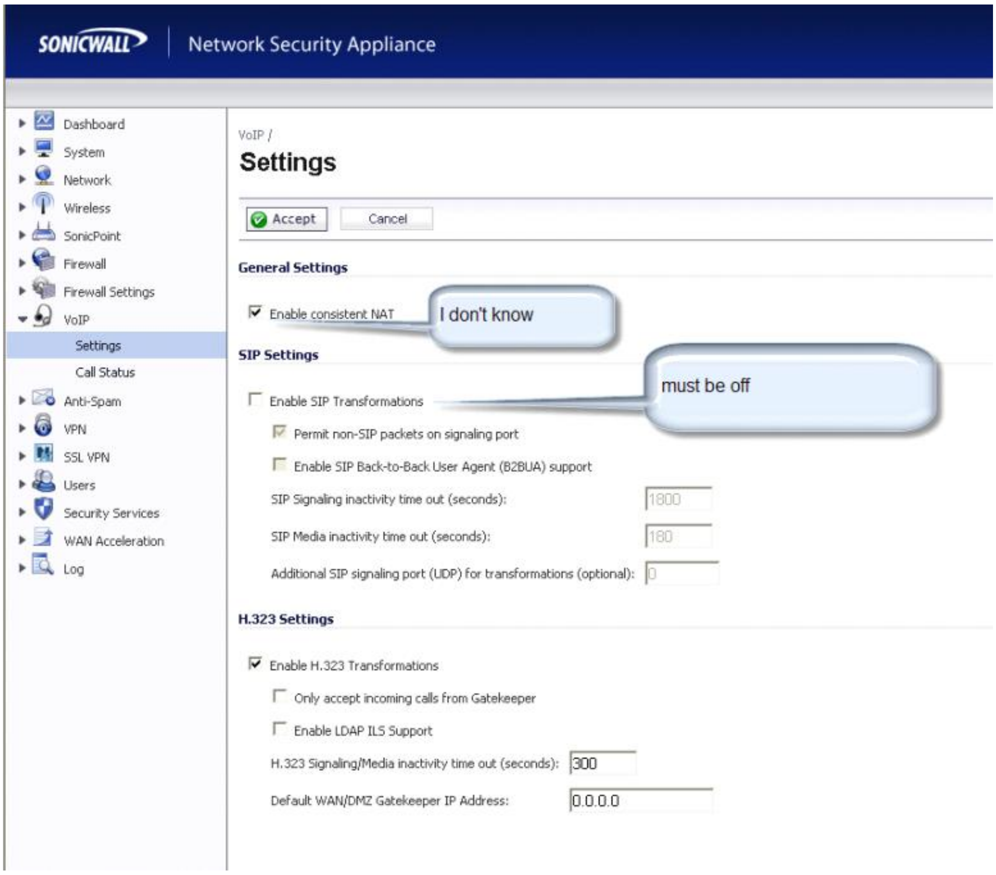
□ Enable IP header checksum enforcement

□ Enable UDP checksum enforcement

UDP

Default UDP Connection Timeout (seconds): 30

Must be >= 180



VoIP /

Settings

General Settings

☑ Enable consistent NAT

I don't know

SIP Settings

□ Enable SIP Transformations

must be off

☑ Permit non-SIP packets on signaling port

□ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 180

Additional SIP signaling port (UDP) for transformations (optional): 0

H.323 Settings

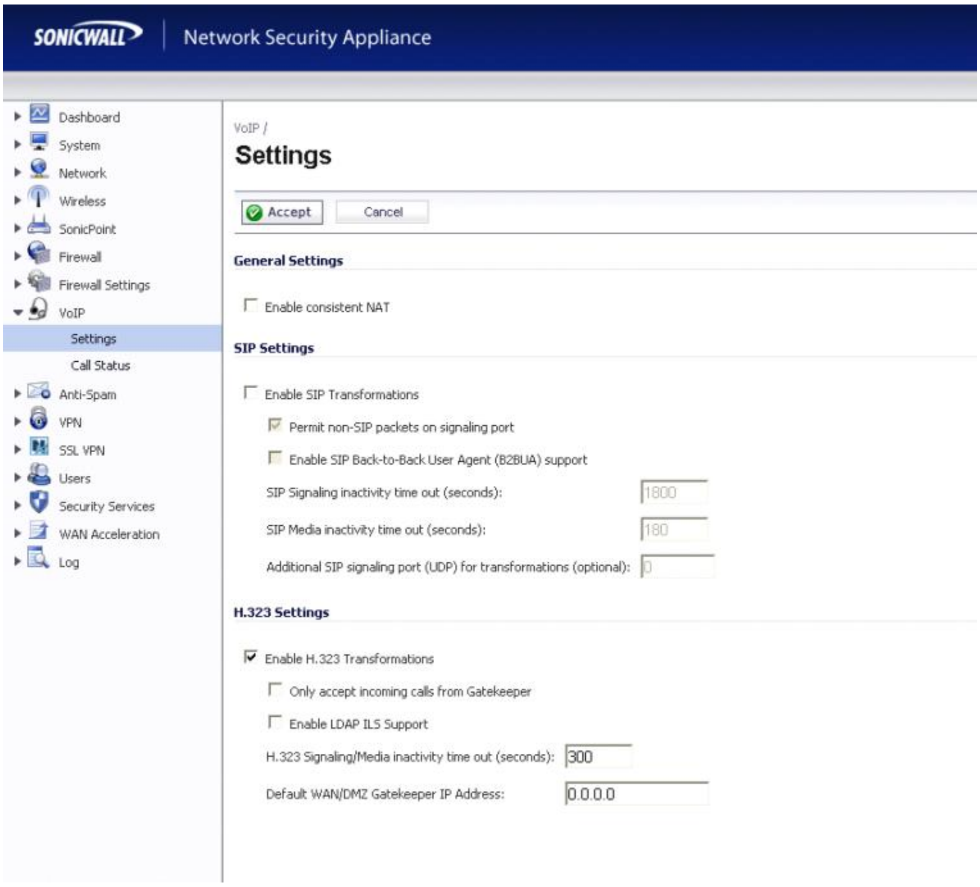
☑ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

□ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0



Settings

General Settings

☐ Enable consistent NAT

SIP Settings

☐ Enable SIP Transformations

☑ Permit non-SIP packets on signaling port

☐ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds): 1800

SIP Media inactivity time out (seconds): 180

Additional SIP signaling port (UDP) for transformations (optional): 0

H.323 Settings

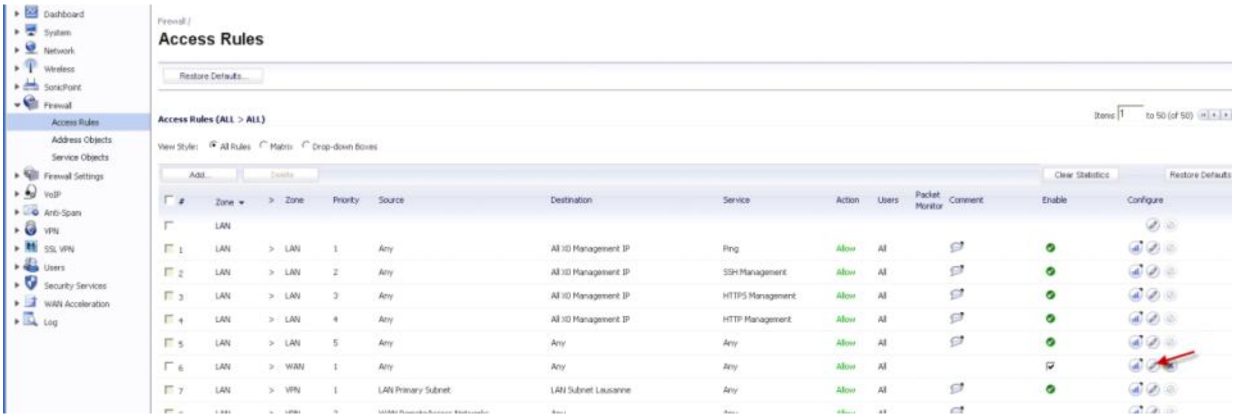
☑ Enable H.323 Transformations

☐ Only accept incoming calls from Gatekeeper

☐ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0



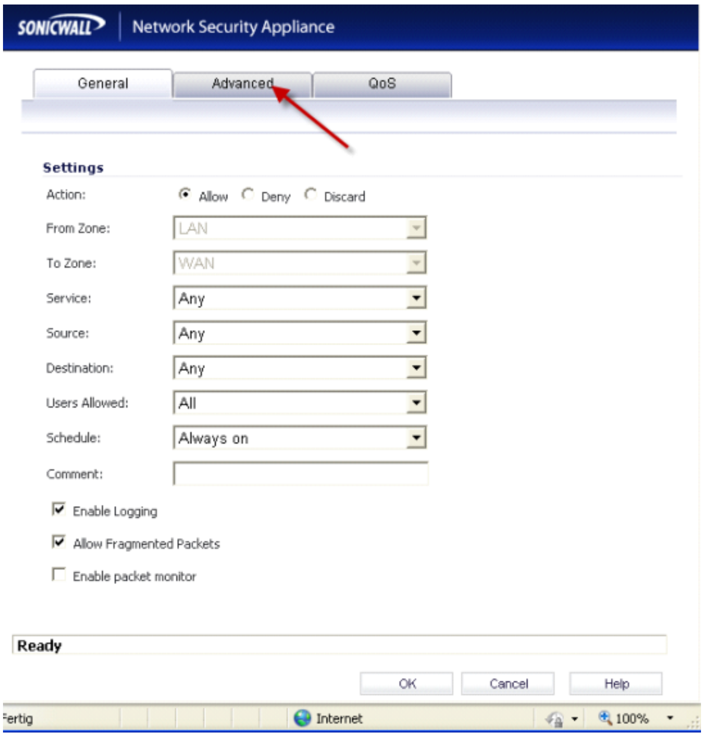
Access Rules

Access Rules (ALL > ALL)

Items 1 to 50 (of 50)

View Style: ● All Rules ○ Matrix ○ Drop-down Boxes

☐ #	Zone	>	Zone	Priority	Source	Destination	Service	Action	Users	Packet Monitor	Comment	Enable	Configure
☐	LAN												
☐ 1	LAN	>	LAN	1	Any	All X0 Management IP	Ping	Allow	All			●	
☐ 2	LAN	>	LAN	2	Any	All X0 Management IP	SSH Management	Allow	All			●	
☐ 3	LAN	>	LAN	3	Any	All X0 Management IP	HTTPS Management	Allow	All			●	
☐ 4	LAN	>	LAN	4	Any	All X0 Management IP	HTTP Management	Allow	All			●	
☐ 5	LAN	>	LAN	5	Any	Any	Any	Allow	All			●	
☐ 6	LAN	>	WAN	1	Any	Any	Any	Allow	All			☑	
☐ 7	LAN	>	VPN	1	LAN Primary Subnet	LAN Subnet Lausanne	Any	Allow	All			●	



Settings

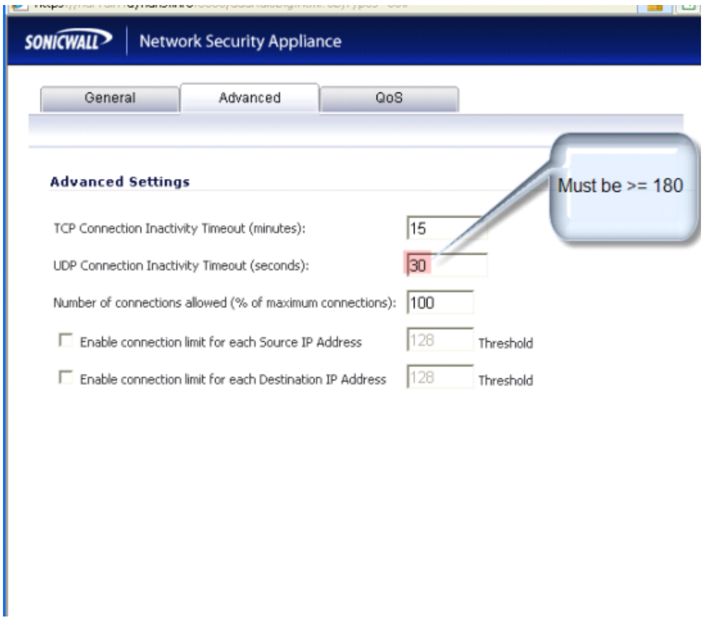
Action:	● Allow ○ Deny ○ Discard
From Zone:	LAN
To Zone:	WAN
Service:	Any
Source:	Any
Destination:	Any
Users Allowed:	All
Schedule:	Always on
Comment:	

☑ Enable Logging

☑ Allow Fragmented Packets

☐ Enable packet monitor

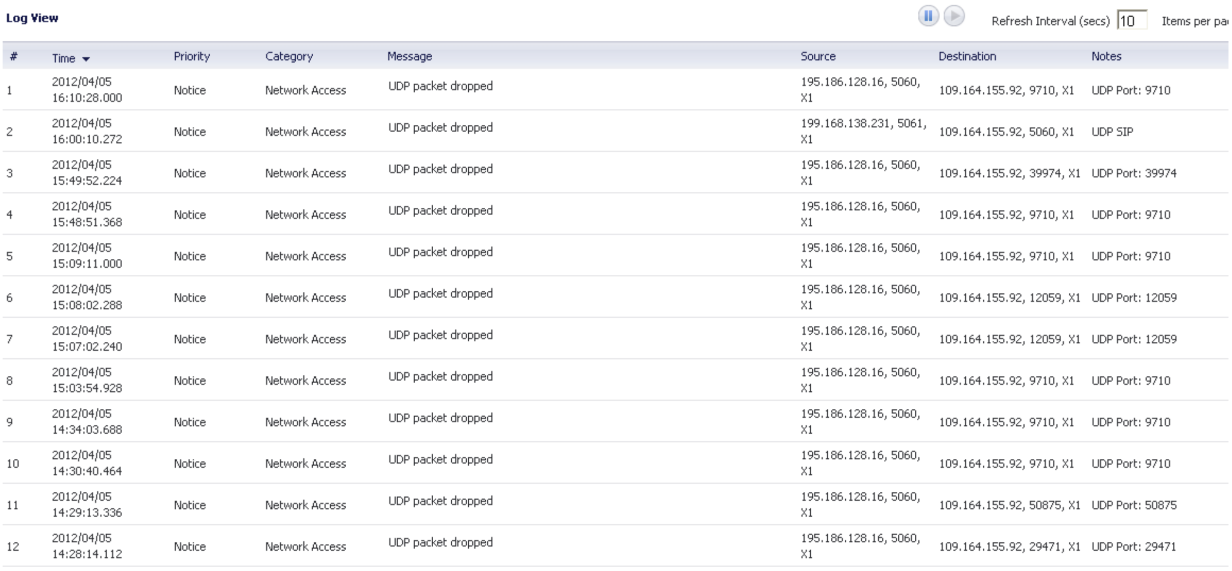
Ready



Advanced Settings

Must be >= 180

TCP Connection Inactivity Timeout (minutes):	15	
UDP Connection Inactivity Timeout (seconds):	30	
Number of connections allowed (% of maximum connections):	100	
☐ Enable connection limit for each Source IP Address	128	Threshold
☐ Enable connection limit for each Destination IP Address	128	Threshold



Log View

Refresh Interval (secs) 10 Items per pa

#	Time	Priority	Category	Message	Source	Destination	Notes
1	2012/04/05 16:10:28.000	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
2	2012/04/05 16:00:10.272	Notice	Network Access	UDP packet dropped	199.168.138.231, 5061, X1	109.164.155.92, 5060, X1	UDP SIP
3	2012/04/05 15:49:52.224	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 39974, X1	UDP Port: 39974
4	2012/04/05 15:48:51.368	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
5	2012/04/05 15:09:11.000	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
6	2012/04/05 15:08:02.288	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 12059, X1	UDP Port: 12059
7	2012/04/05 15:07:02.240	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 12059, X1	UDP Port: 12059
8	2012/04/05 15:03:54.928	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
9	2012/04/05 14:34:03.688	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
10	2012/04/05 14:30:40.464	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 9710, X1	UDP Port: 9710
11	2012/04/05 14:29:13.336	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 50875, X1	UDP Port: 50875
12	2012/04/05 14:28:14.112	Notice	Network Access	UDP packet dropped	195.186.128.16, 5060, X1	109.164.155.92, 29471, X1	UDP Port: 29471