

Konfigurationsübersicht Firewall

Basis: NET.3.2 (Auswahl)

Geräte: _____

Standort: _____

Baustein	Maßnahme	Bedeutung/Umsetzung
NET.3.2.A2	Festlegen der Firewall-Regeln ^{*)}	Gesamte Kommunikation muss über Firewall geleitet werden Keine unerlaubten Verbindungen aus geschütztem Netz heraus
NET.3.2.A3	Einrichten geeigneter Filterregeln am Paketfilter ^{*)}	Müssen geeignete Filterregeln für Paketfilter definiert und eingerichtet haben
NET.3.2.A4	Sichere Konfiguration der Firewall	Konfig muss nachvollziehbar dokumentiert sein. Integrität der Datei muss geschützt werden. Nur zwingend erforderliche Dienste verfügbar
NET.3.2.A6	Schutz der Administrationsschnittstellen	Alle Zugänge (Admin, Management) müssen auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden
NET.3.2.A7	Notfallzugriff auf die Firewall	Es muss immer möglich sein, direkten Zugriff auf die Firewall zu haben (lokal)
NET.3.2.A8	Unterbindung von dynamischem Routing	Dynamisches Routing muss deaktiviert sein, es sei denn, Paketfilter wird mit NET3.1 eingesetzt
NET.3.2.A9	Protokollierung	Abgewiesene Netzverbindungen, fehlgeschlagene Zugänge auf System-Ressourcen, Fehlermeldungen der Firewall-Dienste
NET.3.2.A17	Deaktivierung von IPv4 oder IPv6	Wenn es nicht benötigt wird, sollte es am jeweiligen Firewall-Netzzugangspunkt deaktiviert werden
NET.3.2.A18	Administration über ein gesondertes Managementnetz	Ausschließlich über ein separates Managementnetz administriert
NET.3.2.A28	Zentrale Filterung von aktiven Inhalten	Aktive Inhalte sollten gemäß den Sicherheitszielen der Institution zentral gefiltert werden
*) ggf. gesondert dokumentieren		

Filterregeln				
Nr.	Aktion	Quelle	Ziel	Dienst / Protokoll
1				
2				
3				
4				
(...)	(...)	(...)	(...)	(...)
n+1 ^{**)}	Verbiete	ANY	ANY	ANY