

Im KDN III anzusprechende Namen und IP-Adressen für Dienste der SIDI im SVN 2.0



DNS-Name	IP-Adresse(n)	Bemerkungen
DNS		
dns20.pzd-kdn.de	10.101.1.8	primärer DNS intern
dns21.pzd-kdn.de	10.101.1.9	sekundärer DNS intern
Mail		
mail20.pzd-svn.de	10.101.65.10 10.101.65.11 bis 10.101.65.16	Mailserver der SIDI (für Verkehr Richtung SIDI) dedizierte IP-Adressen der SIDI-Mailserver, nicht für den Wirkbetrieb verwenden! - bitte nur nach Aufforderung zum Troubleshooting verwenden!
HTTP/FTP/SSL-Proxy		
proxy20.pzd-kdn.de	10.101.1.127 10.101.1.13; 10.101.1.14	IP-Adresse Proxyserver dedizierte IP-Adressen der beiden Proxyserver, nicht für den Wirkbetrieb verwenden! - bitte nur nach Aufforderung zum Troubleshooting verwenden! Proxy Port: 8080 (für HTTP, HTTPS/SSL und FTP), für natives FTP: Port 21
NTP		
ntp20.pzd-svn.de	10.101.64.50	NTP-Server1
ntp21.pzd-svn.de	10.101.64.51	NTP-Server2
WSUS		
wsus20.pzd-svn.de	10.101.64.40	Windows Software Update Service WSUS kann nur von dezentralen WSUS-Servern genutzt werden
BlackBerry		
-	10.101.218.9	BlackBerry-Portforwarding für alle BES-Versionen
-	10.101.218.8	zusätzliches BlackBerry-Portforwarding ab BES-Version 10
-	10.101.218.7	zusätzliches BlackBerry-Portforwarding ab BES-Version 12

Hinweis: Bitte verwenden Sie bei der Konfiguration Ihrer Anwendungen die DNS-Namen der Server und nicht die IP-Adressen (ausser natürlich beim DNS)

Folgende Regeln müssen auf vorhandenen Firewallsystemen beim Nutzer für die Kommunikation mit den Basisdiensten der SIDI freigegeben werden

Dienst	Quelle	Ziel	Protokoll	Bemerkung
DNS	DNS-Clients vom Nutzer, DNS-Server beim Nutzer	Nameserver SIDI: 10.101.1.8, 10.101.1.9	DNS (UDP Port 53, TCP Port 53)	Nameserverabfragen, Zonentransfers
DNS	Nameserver SIDI: 10.101.1.8, 10.101.1.9	DNS-Server Nutzer	DNS (UDP Port 53, TCP Port 53)	Zonentransfers, Diagnose
Mail	Mailserver vom Nutzer	In-Mailserver SIDI: 10.101.65.10, 10.101.65.11, 10.101.65.12, 10.101.65.13, 10.101.65.14, 10.101.65.15, 10.101.65.16	SMTP (TCP Port 25)	Mailverkehr ausgehend in Richtung Mailserver der SIDI (für den regulären Mail-Betrieb muß nur die IP 10.101.65.10 freigeschaltet sein, die restlichen angegebenen IP-Adressen nur rein vorsorglich für Fehlersuche/Troubleshooting freischalten)
Mail	Mailserver SIDI: 10.101.65.11, 10.101.65.12, 10.101.65.13, 10.101.65.14, 10.101.65.15, 10.101.65.16	Mailserver beim Nutzer	SMTP (TCP Port 25)	Mailverkehr eingehend aus Richtung Ausgangs-Mailserver der SIDI
HTTP/FTP-Proxy	Proxyserver des Nutzers, Clients beim Nutzer (Browser, FTP-Clients)	Proxyserver SIDI: 10.101.1.127, 10.101.1.13, 10.101.1.14	HTTP (TCP Port 8080), FTP (TCP Port 21)	Zugriff vom Nutzer aus auf zentralen HTTP-Proxy SIDI, Zugriff auf nativen FTP-Proxy (für den regulären Mail-Betrieb muß nur die IP 10.101.1.127 freigeschaltet sein, die restlichen angegebenen IP-Adressen nur rein vorsorglich für Fehlersuche/Troubleshooting freischalten)
HTTP/FTP-Proxy	Proxyserver SIDI: 10.101.1.13, 10.101.1.14	Webserver beim Nutzer	HTTP (TCP Port 80), HTTPS (TCP Port 443), FTP (TCP Port 21)	Zugriff auf den/die Webserver vor Ort beim Nutzer vom zentralen Proxy der SIDI aus (für Webangebote des Nutzers im KDN-Intranet)
Reverse-Proxy	Reverse-Proxy SIDI: 10.101.67.11, 10.101.67.12, 10.101.67.13, 10.101.67.14	Webserver beim Nutzer	HTTP (TCP Port 80), HTTPS (TCP Port 443)	Zugriff vom Reverse-Proxy der SIDI aus auf Webserver beim Nutzer (für Webangebote des Nutzers im Internet)
NTP	NTP-Clients Nutzer	NTP-Server SIDI: 10.101.64.50, 10.101.64.51	NTP (UDP Port 123)	Zugriff auf zentralen NTP-Dienst
WSUS	WSUS beim Nutzer	WSUS SIDI: 10.101.64.40	HTTP (TCP Port 80), HTTPS (TCP Port 443)	Zugriff von dezentralen WSUS-Servern auf zentralen WSUS
BlackBerry	BES beim Nutzer	Portforwarding SIDI: 10.100.218.9 10.100.218.8 10.100.218.7	TCP Port 3101	Zugriff auf die BlackBerry - Infrastruktur der Region EMEA 10.101.218.9 wird für alle BES-Versionen benötigt 10.101.218.8 wird ab BES-Version 10 zusätzlich benötigt 10.101.218.7 wird ab BES-Version 12 zusätzlich benötigt
ICMP	Netzwerk beim Nutzer	ANY (bzw. alternativ: SIDI: 10.101.0.0/16, KDN-WAN: 10.97.0.0/16, RAS-KDN: 10.48.0.0/14, Extranet: 10.200.128.0/17, DOI/NdB: 10.168.0.0/16, Land: 172.16.0.0/12)	ICMP (Typ 0, 3, 4, 8, 11, 12)	Netzwerk-Betrieb + Troubleshooting (Echo Request (8), Echo Reply (0), Destination Unreachable (3), Source Quench (4), Time Exceeded (11), Parameter Problem (12). Die in Klammern stehende Nummer identifiziert hierbei den betreffenden ICMP-Meldungstyp.)
ICMP	ANY (bzw. alternativ: SIDI: 10.101.0.0/16, KDN-WAN: 10.97.0.0/16, RAS-KDN: 10.48.0.0/14, Extranet: 10.200.128.0/17, DOI/NdB: 10.168.0.0/16, Land: 172.16.0.0/12)	Server bzw. Client beim Nutzer	ICMP (Typ 0, 3, 4, 8, 11, 12)	Netzwerk-Betrieb + Troubleshooting (Echo Request (8), Echo Reply (0), Destination Unreachable (3), Source Quench (4), Time Exceeded (11), Parameter Problem (12). Die in Klammern stehende Nummer identifiziert hierbei den betreffenden ICMP-Meldungstyp.)

Für die Nutzung zusätzlicher Dienste (z.B. RAS-Dienst, DOI/NdB, Blackberry etc.) müssen bei Bedarf ggf. weitere Regeln erstellt werden.

Die oben aufgeführten Regelsätze gelten für Firewallsysteme, die ein stateful Inspection unterstützen (üblicherweise alle modernen Firewallsysteme). Sollte das nicht der Fall sein (z.B. Einsatz eines statischen Paketfilters), so müssen die Regelsätze entsprechend ergänzt werden (u.a. TCP-Rückverbindungen, FTP-Data-Kanal)

Freischaltung Mailserver

Bitte gewährleisten Sie bei der Konfiguration Ihres lokalen Mailserver, dass dieser eingehende Mail von den zentralen Mailservern der SIDI annimmt (z.B. Hinzufügen der Mailserver der SIDI zu den vertrauten (trusted) Hosts, ggf. Access-Listen modifizieren etc.).