SINA®
SOLID

Krisensichere Netze – Resilienz durch Vollvermaschung

VPN-Automatisierung für SINA

secunet.com

Wenn der Bagger das Glasfaserkabel durchtrennt …

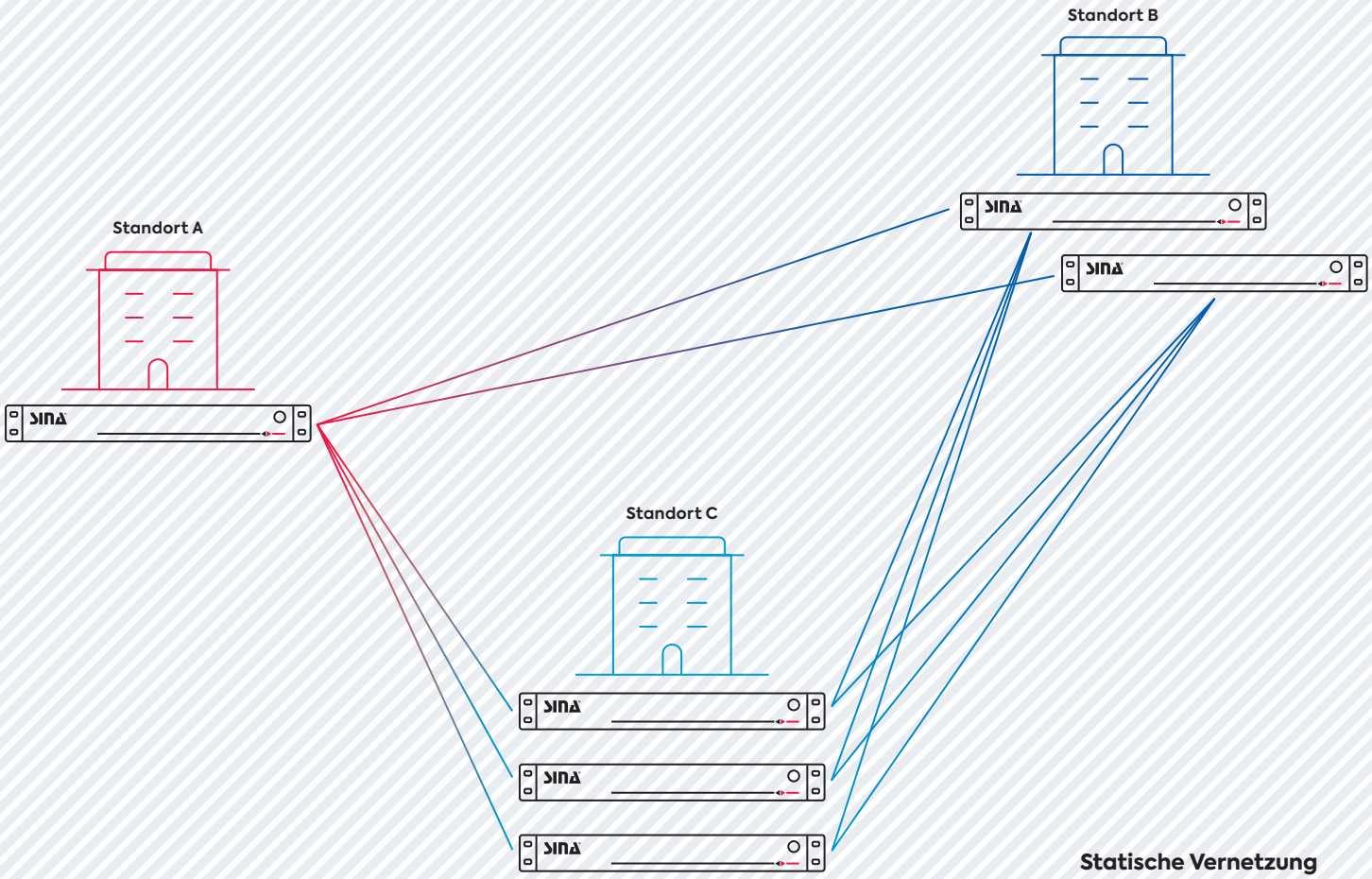
Ein bekannter Vorfall: Tausende Passagiere müssen wegen einer globalen IT-Panne bei einer großen Fluggesellschaft Verspätungen und Flugausfälle hinnehmen. Zumindest die Ursache war schnell erkannt: Ein Bagger hatte im Rahmen von Bauarbeiten an einer Bahnstrecke unweit eines großen deutschen Flughafens mehrere Glasfaserkabel durchtrennt.

Gründe für einen Netzausfall gibt es viele – und sei es lediglich wegen einer Panne bei Bauarbeiten. Die Folgen sind allerdings oftmals weitreichend. Das können bei einer Airline wie im obigen Beispiel Störungen im Flugbetrieb sein. Genauso kann es eine Behörde treffen, die beispielsweise keine Service-Angebote mehr für Bürger*innen bereitstellen kann.

Es ist daher unerlässlich, Netzwerke möglichst zukunfts- und krisensicher aufzubauen. Denn eine stabile Verbindung ist letztlich auch elementar für die Arbeitsfähigkeit der Mitarbeiter*innen. Das kann für Behörden und Unternehmen mit erhöhten Sicherheitsbedarf allerdings eine echte Herausforderung darstellen.

Krisenanfälligkeit statischer Netzwerke

Mit VPN-Gateways, wie der SINA L3 Box S, können Netze über mehrere Standorte mit IPsec abgesichert werden. Zudem sorgen die Gateways dafür, dass Mitarbeiter*innen mit ihren Endgeräten sicher an das Intranet angebunden werden und auf interne Dienste zugreifen können.



Statische Vernetzung

Bricht die direkte Verbindung zwischen zwei Standorten weg, weil zum Beispiel – wie im eingangs beschriebenen Fall – das Glasfaserkabel versehentlich bei Bauarbeiten durchtrennt wurde, können Mitarbeiter*innen der betroffenen Standorte nicht mehr auf die Server des anderen Standorts zugreifen. Je nach Standort können von der Störung auch wichtige zentrale Dienste wie Telefonie betroffen sein. Aufgrund der gewachsenen Komplexität der Netze und der geografischen Verteilung der Dienste sind in der Praxis trotz bester (manueller) Planung solche Krisen keine Einzelfälle.

Aber auch unabhängig vom Krisenfall: diese manuelle und statische Konfiguration der Netzwerke ist kostenintensiv und potentiell fehleranfällig.

Was ist SINA?

Mit der Sicheren Inter-Netzwerk-Architektur SINA können Mitarbeiter*innen von Behörden oder Unternehmen sicher mit sensiblen oder gar eingestuften Informationen umgehen – innerhalb oder außerhalb des Büros. Perfekt aufeinander abgestimmte Netzwerkkomponenten und Clients sorgen für eine wirksame Verschlüsselung und Trennung unterschiedlich klassifizierter Daten sowohl lokal als auch beim Transfer über offene Netze.

Automatisches Routing

SINA SOLID löst die Probleme statischer Konfigurationen, indem es die optimale Datenverbindung im Netz aufbaut. SOLID steht dabei für „Secure Over-Lay for IPsec Discovery“ und sorgt für ein automatisches Routing bei IPsec-VPN-Verbindungen. Dabei bleiben die Sicherheitseigenschaften von IPsec und SINA vollständig erhalten.

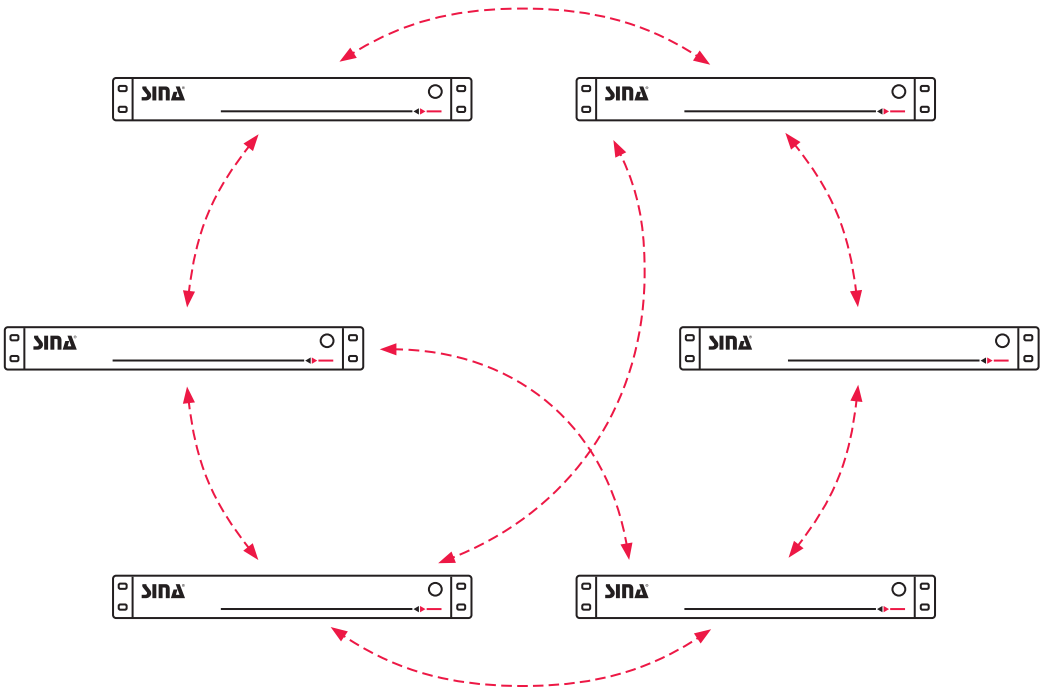
Georedundante Cluster

SINA SOLID macht zudem jeden Standort Cluster-fähig, d. h. stellt einen Hot-Stand-by ähnlichen Verbund bereit, indem alle SINA L3 Boxen in Bereitschaftsfunktion sind, falls Systeme ausfallen. Diese Cluster können auch über mehrere lokal voneinander entfernte Standorte verteilt werden, sodass georedundante Cluster die Ausfallsicherheit erhöhen. (Externe) Loadbalancer werden damit nicht mehr benötigt.

Wenn die Verbindung zwischen zwei Standorten unterbrochen wird, routet die SOLID-Technologie automatisch innerhalb von wenigen Sekunden um, ohne dass die Administration manuell tätig werden muss. Ist die direkte Verbindung zwischen Standort A und Standort B unterbrochen, wird somit der Datenverkehr zwischen A und B über Standort C umgelenkt. Das Netz reagiert dabei eigenständig dynamisch auf die Änderungen. Routinginformationen werden im Netz selbst gehalten und regelmäßig optimiert.

Die automatische, optimale Krypto-Routenfindung funktioniert auch, wenn neue Strecken, Standorte und Geräte hinzukommen. Wenn beispielweise eine neue SINA L3 Box S in Betrieb genommen wird, organisiert sich daraufhin das Netz selbst neu.

Mit SINA SOLID wird somit der Verwaltungsaufwand bei großen und komplexen Netzen erheblich reduziert.



Die Koordination der VPN-Vermaschung übernimmt das transparente und gesicherte Overlay-Netzwerk selbst. Es steuert die dynamische Anordnung aller SINA L3 Boxen in einem logischen Ring.

Optimal vernetzt

Wie die SINA Workstation S von der SOLID-Technologie profitiert.

Bestmögliche Client-Anbindung

Die Vorteile von SINA SOLID stehen bereits seit einiger Zeit für die SINA L3 Box S zur Verfügung. Nun können die beschriebenen Vorteile von auch für die SINA Workstation S genutzt werden. Die SOLID-Technologie optimiert somit nicht nur die Standortvernetzung – auch SINA Workstations werden (quasi wie ein mobiler Standort) automatisch bestmöglich im Netz angebunden. Das ist insbesondere im Krisenfall von Vorteil.

Denn üblicherweise läuft sämtlicher Datenverkehr über die zentralen Zugangsgateways. Das ist bei einem zentralen Systemausfall problematisch. Sind diese trotz vorhandener Redundanzen nicht erreichbar, können sich Mitarbeiter*innen nicht mehr mit dem Intranet verbinden oder keine zentralen Dienste mehr nutzen.

Cleveres Routing statt Nadelöhr

Mit SINA SOLID hingegen können sich die SINA Workstations auch mit einem georedundanten Cluster eines anderen Standorts verbinden. Denn die zentralen Zugänge müssen mit SINA SOLID nicht mehr zwangsläufig passiert werden. Der Weg kann über alle zur Verfügung stehenden SINA L3 Boxen gehen, je nachdem welcher Pfad aktuell der beste ist. Da es viele potenzielle Wege gibt, entsteht kein zentrales Nadelöhr. Bei dem ständig zunehmenden Datenverkehr ist das ein wichtiger Schritt hin zu mehr Resilienz.

Entwickelt in universitärer Forschung

SINA SOLID entstand aus einer preisgekrönten Forschungskooperation mit der Technischen Universität Ilmenau. Die zentrale Idee des Ilmenauer Forscherteams an der Fakultät für Informatik und Automatisierung war es, die Gateways in einer Ringstruktur mit zusätzlichen Querverbindungen anzuordnen, sodass auch indirekte Szenarien (SINA L3 Box S hinter SINA L3 Box S) unterstützt werden. Nach ersten Erfolgen im Jahr 2010 und mehrjähriger Entwicklungszeit, erhielt SINA SOLID bereits 2017 die Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-NfD.

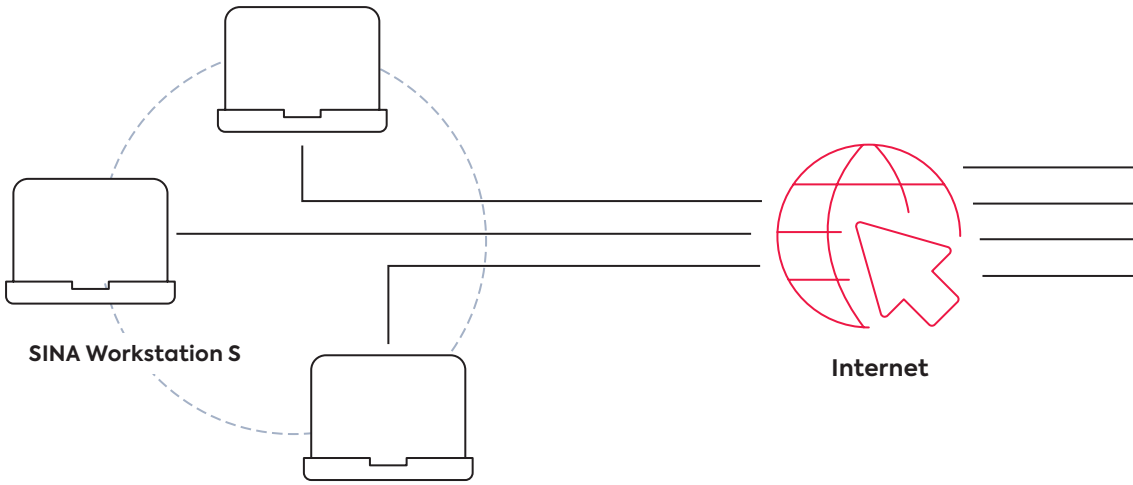
In einem weiteren Forschungsprojekt mit der TU Ilmenau wurde für eine beschleunigte Netzwerkverschlüsslung HEAT (High-Speed Encryption Acceleration Track) entwickelt. Die Kryptobeschleunigung wird mit SINA SOLID für die SINA L3 Box S aktiviert.

Peer-to-Peer-Kommunikation für die Workstation

Ganz neue Möglichkeiten eröffnen sich darüber hinaus für die Kommunikation der SINA Workstations S untereinander. Denn SINA SOLID ermöglicht die Direktverbindung (Peer-to-Peer) zwischen den Geräten. Das entlastet zum einen die zentralen Zugänge, da Telefonie- und Videodaten nicht mehr durch einen Engpass müssen.

Zum anderen macht dies das Netz auch robuster bei Ausfällen. Selbst wenn die Verbindung zwischen den Standorten unterbrochen wird, können die SINA Workstations weiterhin miteinander kommunizieren. Entsprechend konfiguriert bleiben bestehende bilaterale (Video-)Telefonieverbindungen aufrechterhalten.

Peer-to-Peer-Anwendungen, die ohne einen zentralen Server funktionieren, können weiter genutzt werden. Somit ist auch der Aufbau einer neuen Verbindung prinzipiell möglich. Die Funktion bietet daher viel Potential für Lösungen, die eine Krisenkommunikation bei einem zentralen Serverausfall unterstützen.



Peer-to-Peer-Kommunikation und dezentrale Serverzugriffe

Resilienz dank Vollvermaschung

Mit SINA SOLID entsteht eine Vollvermaschung des VPN-Netzwerks. Diese macht das Netz krisensicher bei Ausfällen und Engpässen. Verbindungen werden automatisch in unter zehn Sekunden von anderen VPN-Gateways übernommen, wenn Geräte ausfallen.

Auch Sabotage durch Denial-of-Service-Angriffe (DoS-Angriffe), bei denen Server gezielt mit Anfragen bombardiert werden, bis sie zusammenbrechen, wird durch die SOLID-Technologie erschwert.

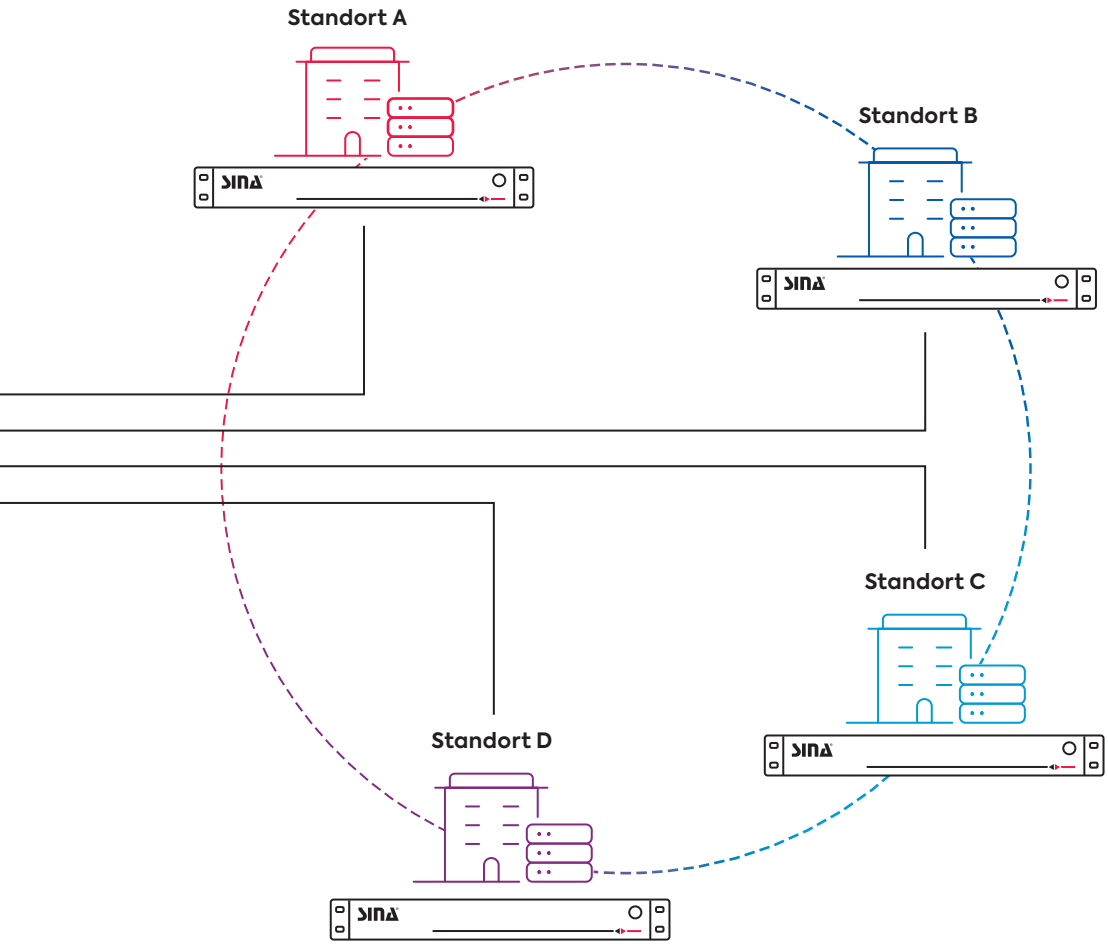
SINA SOLID ist das erste Produkt für dynamische und automatisierte VPN-Vollvermaschung, das eine Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erhalten hat. Die Flexibilität der Lösung bei gewohnt hohem Sicherheitsniveau der Datenübertragung und angeschlossenen Systeme macht SINA SOLID einzigartig auf dem Markt.

Den Überblick behalten mit SINA Monitoring

Zahlreiche Fehler- und Ausfallsituationen werden durch SINA SOLID bereits automatisch behandelt und ihren Folgen abgemildert. Dennoch gibt es Situationen, bei denen manuelle Maßnahmen nötig sind, beispielsweise wenn Geräte ausgetauscht oder Leitungen repariert werden müssen.

In der Produktfamilie knüpft hier das SINA Monitoring an, das zur Betriebsüberwachung der SINA Komponenten entwickelt wurde. Es bietet dabei nicht nur eine optimale Einsicht in den aktuellen Netzzustand, sondern alarmiert auch bei Störungen und stellt entsprechende Diagnosewerkzeuge bereit.

Das Overlay-Netzwerk liefert dazu wertvolle Daten für eine Überwachung von SINA SOLID in Echtzeit, die mit dem SINA Monitoring optimal aufbereitet und analysiert werden können.



SINA SOLID...

- reduziert die Betriebsaufwände in großen und komplexen Netzen durch automatische Optimierung und Konfiguration
- macht Boxen und Cluster mandantenfähig
- erspart die Loadbalancer für Boxen-Cluster durch automatische Verteilung von IPsec-Verbindungen auf die verfügbaren SINA L3 Boxen
- übernimmt bei Ausfall automatisch laufende Verbindungen auf andere Boxen in unter zehn Sekunden
- erleichtert Kapazitätsmanagement und Troubleshooting durch Echtzeit-Monitoring der SINA L3 Boxen und Clients

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen.
Das Unternehmen wurde 1997 gegründet. Es ist an der Deutschen Börse gelistet und erzielte 2023 einen Umsatz von rund 393 Mio. Euro.

secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

Weitere Informationen:
secunet.com/sina

secunet

Broschüre_SINA SOLID_DE_02/2024