

SINA SOLID – Prämierte und patentierte Lösung für eine sichere dynamische VPN-Vernetzung

Die einzigartige Technologie SINA SOLID (Secure OverLay for IPsec Discovery) ist eine neue Funktion für die SINA L3 Box und das erfolgreiche Ergebnis eines mehrjährigen Forschungsprozesses. SINA SOLID kann sehr große und flexible IPsec-Netze automatisiert konfigurieren und steigert dabei deutlich auf höchstem Sicherheitsniveau die Performance.

Die Funktion erlaubt eine dynamische VPN-Vernetzung, die automatisch die Verbindung zwischen den einzelnen Netzknotenpunkten konfiguriert. Dabei bleiben alle Sicherheitseigenschaften von IPsec und SINA vollständig erhalten. Mit SINA SOLID wird der Verwaltungsaufwand bei großen und komplexen Netzen erheblich reduziert, da das System selbsttätig auf Änderungen im Netzwerk reagiert und ein manuelles Eingreifen nicht mehr erforderlich ist.

VPN (virtuelle private Netzwerke) auf Basis von IPsec bieten einen weitreichenden Schutz gegen Angriffe auf die Vertraulichkeit und Integrität übertragener Daten. Wegen ihrer komplexen und oft statischen Konfiguration ist jedoch die Integration neuer IPsec-Gateways in ein Netzwerk oder die Anpassung von Routen im VPN oft mit größerem Aufwand verbunden. In der Regel erfolgt die Konfiguration der häufig dazu eingesetzten IPsec-Infrastrukturen manuell. Das bedeutet, selbst bei großen Netzwerken werden zwischen den beteiligten IPsec-

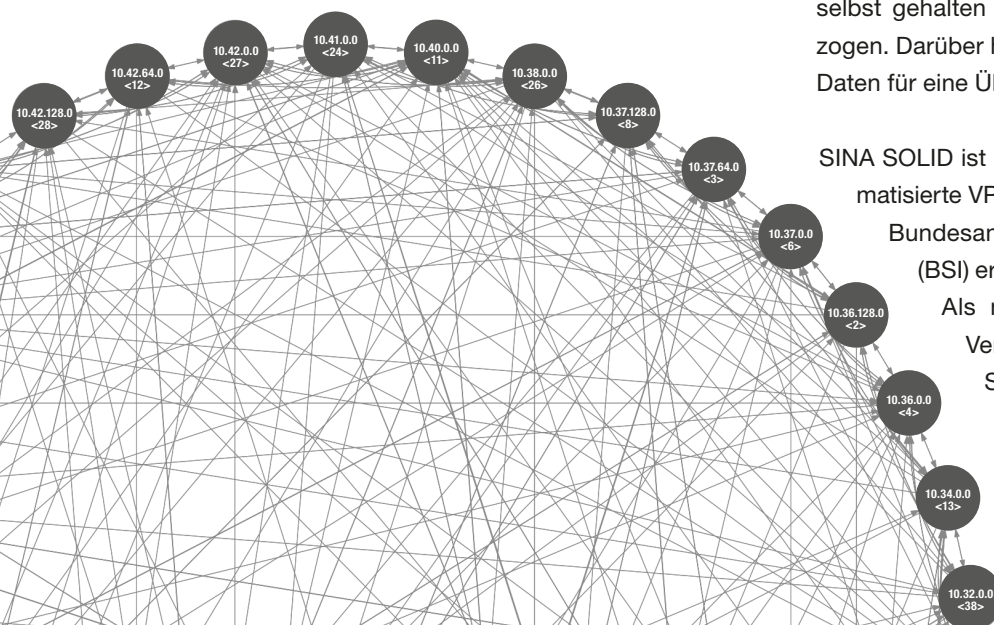
Gateways paarweise Sicherheitsbeziehungen eingerichtet. Dieses Verfahren, bei dem der Aufwand mit der Anzahl der IPsec-Gateways quadratisch wächst, kann kostenintensiv werden und potenziell fehleranfällig sein. Die Verfügbarkeit des Netzes und die Betriebskosten für zentrale Knotenpunkte sind ausschlaggebende Kriterien für die Etablierung von VPN. Bisher erhielt noch kein Produkt für dynamische und automatisierte VPN-Vollvermaschung eine Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

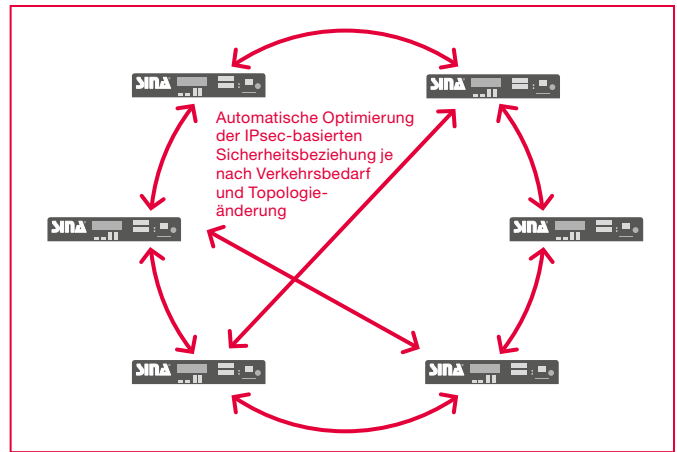
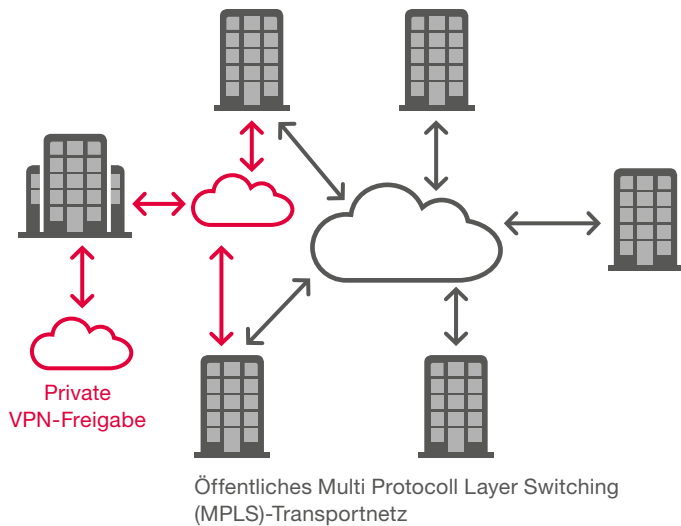
SINA SOLID ermöglicht die dynamische VPN-Vermaschung durch automatisierte Konfiguration für große bis sehr große Netz-Infrastrukturen. Es reagiert auf Topologieänderungen und Wegeredundanz zur Laufzeit. Vor allem bei komplexen, potentiell stark vermaschten VPN-Topologien kann dadurch der Verwaltungsaufwand gering gehalten werden. Dabei ist ein schneller Kommunikationsaufbau gewährleistet. Zudem wird die Sabotageresistenz gegenüber Denial-of-Service-Angriffen (DoS-Angriffen) gesteigert und erlaubt durch selbstoptimierende Wegewahl zwischen SOLID-Knoten eine dynamische Reaktion auf Ausfälle.

Die Koordination der VPN-Vermaschung übernimmt das transparente und gesicherte Overlay-Netzwerk selbst. Es steuert die dynamische Anordnung aller VPN-Teilnehmer in einem logischen Ring und ermöglicht allen Knoten die Suchanfragen zum Aufbau von Sicherheitsbeziehungen. Alle Routinginformationen werden somit von den VPN-Knoten selbst gehalten und einer regelmäßigen Optimierung unterzogen. Darüber hinaus liefert das Overlay-Netzwerk wertvolle Daten für eine Überwachung von SINA SOLID in Echtzeit.

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 und ist seit Anfang 2017 verfügbar. Als neues Feature wird es mit der Software-Version 3.9 für die SINA L3 Box S bereitgestellt. SINA SOLID gehört somit zu den zentralen IT-infrastrukturellen Kernkomponenten der SINA Produktwelt.

Der SINA SOLID Netzverbund





Dynamische IPsec-basierte Sicherheitsbeziehungen im Overlay-Ringnetz durch Autokonfiguration

Die Vorteile von SOLID

■ Autokonfiguration

- >> Senkung des Konfigurations- und Verwaltungsaufwandes
- >> Sicherheitsbeziehungen werden automatisch konfiguriert
- >> Routing-Informationen werden im Netz selbst gehalten
- >> Topologieänderungen erfolgen dynamisch zur Laufzeit
- >> Dynamische Vermaschung nach Verkehrsbedarf
- >> SOLID trennt die Knoten innerhalb des Verbundes gemäß organisatorischer Vorgaben

■ Hochverfügbarkeit

- >> Clusterbildung durch SOLID vor zentralen Infrastrukturknoten
- >> Redundante Wegwahl zur Laufzeit im SOLID-Verbund
- >> Hohe Sabotageresistenz durch Wegfall zentraler Konzentratoren
- >> Dynamische Reaktion des Netzes auf Knotenausfall
- >> Toleriert Netz-Partitionierung, Verbindungsprobleme und hohe Paketverlusten des zugrundeliegenden Netzwerks

■ Performance

- >> Lastverteilung innerhalb des SOLID-Clusters
- >> Hocheffiziente Wegwahl für Skalierbarkeit in großen VPNs (>1000 Knoten)
- >> Schneller Verbindungsaufbau für VoIP-Szenarien

■ Sicherheit

- >> Ganzheitliches IT-Sicherheitskonzept der SINA L3 Box S
- >> Gehärtete und evaluierte SINA OS-Systemplattform
- >> Smartcard-Technologie
- >> Zulassungskonform konfigurierte Software und BSI-Funktionalitäten
- >> Hohe Sabotageresistenz gegenüber Angriffen durch den innovativen SOLID-Protokollstack

■ Monitoring

- >> Das dynamische SOLID-Overlay erzeugt einen globalen Überwachungsstatus aller Boxen
- >> Automatische Ticketerzeugung inklusiver semantischer Aggregation und Visualisierung
- >> Transparente Kopplung an bestehende Umbrella-Monitoring-Systeme

Die Entwicklung der SINA SOLID Komponente

SINA SOLID entstand aus einer preisgekrönten Forschungskoooperation mit der Technischen Universität in Ilmenau. Erste Erfolge konnten bereits im Jahr 2010 erzielt werden. Nach mehrjähriger Entwicklungszeit hat SINA SOLID die Produktreife erhalten. Gleichzeitig ist die BSI-Zertifizierung für VS-NfD seit Anfang 2017 verfügbar.

Durch die automatisierte Konfiguration von Sicherheitsbeziehungen verbessert SINA SOLID den bisherigen VPN-Ansatz. Freiwerdende Administrations-Ressourcen können nun anderweitig genutzt werden, ohne die Fehleranfälligkeit der Systeme zu erhöhen. Der SOLID-Cluster verspricht darüber hinaus Ausfallsicherheit und hohen Durchsatz. Insbesondere große Infrastrukturen können durch SINA SOLID komplexe Regelwerke vereinfachen, und das unter Beibehaltung der IT-Sicherheit im Sinne der BSI-Zulassung für VS-NfD.

Mehr Informationen: David Ristow | david.ristow@secunet.com