SINA Management

Zentral administrieren

Komfortable Verwaltung aller SINA Komponenten und Benutzer

Das SINA Management verwaltet und konfiguriert zentral alle Komponenten des SINA Produktportfolios: SINA Leitungsverschlüsseler und Gateways, SINA Clients und SINA Workflow. Die zu schützenden Netze werden mit Hilfe des SINA Managements strukturiert aufgebaut, konfiguriert und administriert.

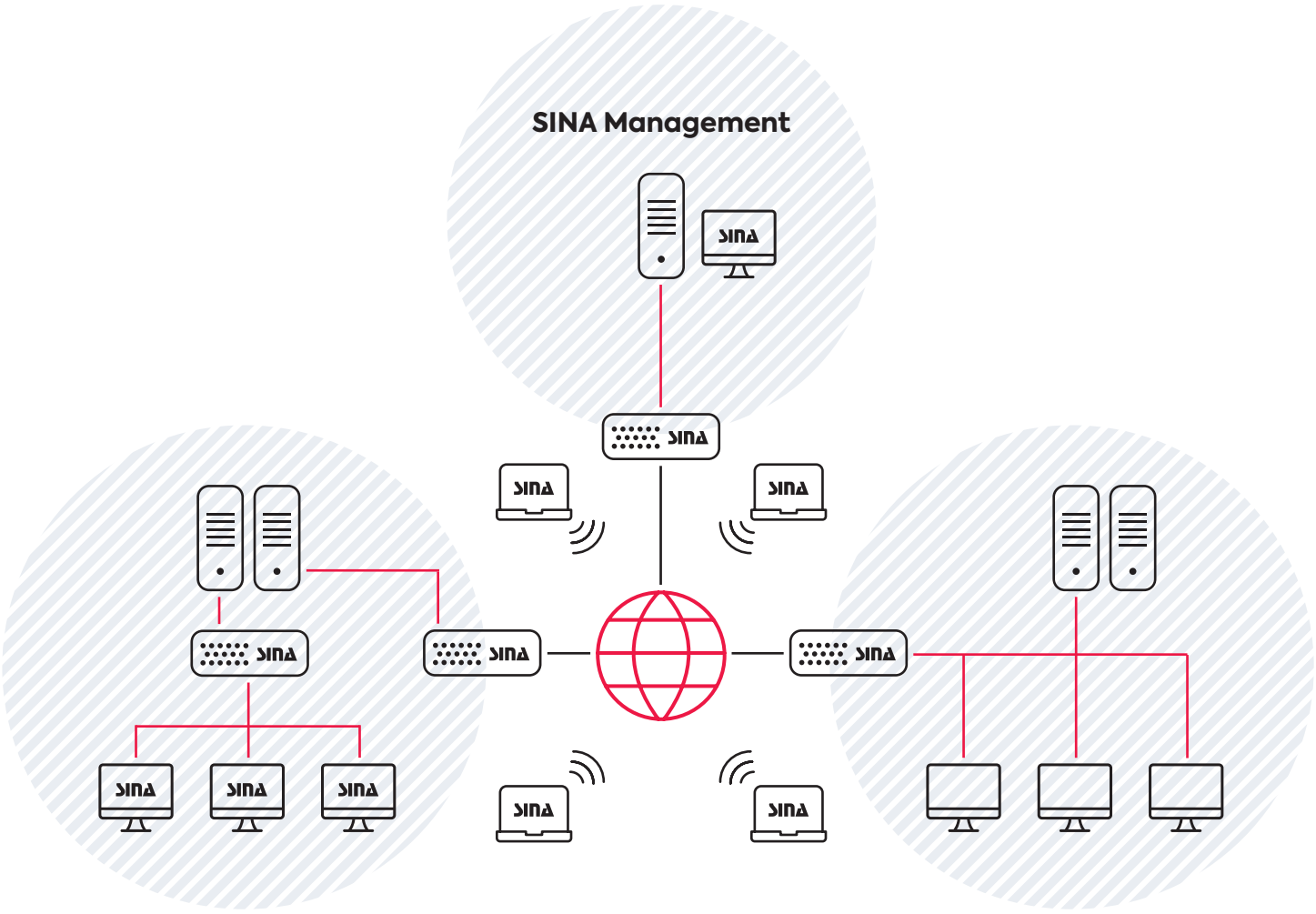
Die graphische Benutzeroberfläche ermöglicht die einfache Konfiguration der Sicherheitsbeziehungen und Zugangsberechtigungen zwischen den SINA Komponenten und Netzen.

Funktionsweise des SINA Managements

Das SINA Management verwaltet Konfigurationsdaten, wie z. B. IP-Adresskonfigurationen oder Routing-Informationen der SINA Komponenten und schreibt diese auf den SINA ID Token – ein vertrauenswürdiges und geschütztes Speichermedium (Smartcard, Security Token oder USB-Token mit integrierter Smartcard). Auf den SINA ID Token werden die Konfigurationsdaten sicher gespeichert und stehen den SINA Komponenten zur Verfügung. Weiterhin werden die für den sicheren Betrieb der Komponenten erforderlichen Schlüssel und Zertifikate im SINA Management erzeugt, verwaltet und ebenfalls auf die Speichermedien geschrieben.

Mit dem SINA Management werden Infrastrukturen mit bis zu mehreren tausend SINA Geräten verwaltet. Dabei sind exemplarisch folgende Parameter bzw. Leistungsmerkmale konfigurierbar:

- Netzwerkkonfiguration von SINA Komponenten
- Sicherheitsbeziehungen und deren Verteilung über einen Verzeichnisdienst
- Sperrlisten kompromittierter bzw. entsprechend gefährdeter Komponenten sowie nicht mehr zuständiger SINA Administratoren
- Kryptographische Algorithmen und Parameter (z. B. Schlüssellebensdauer) für Sicherheitsbeziehungen
- Sichere Online-Updates kryptographischer Parameter sowie der Gerätekonfiguration
- Erzeugung von Authentifizierungsschlüsseln für SINA L2 Boxen
- Ausstellung und Online-Update von Signatur- und Verschlüsselungszertifikaten für SINA Gateways und Benutzer
- Ausstellung von Signatur- und Verschlüsselungszertifikaten für den Einsatz in SINA Workflow



- Anwendungsspezifische Nutzerprofile für (Terminal-)Serverzugriffe
- Konfigurationsprofile für SINA Clients
- Medien-spezifische Zugriffskontrolllisten (ACLs) für die Kontrolle externer Schnittstellen (z. B. USB)
- Sichere Online-Software-Updates von SINA Komponenten

Das SINA Management kann auf den SINA Komponenten über das Netzwerk bestimmte Aktionen initiieren, u. a. Zertifikats-Updates, das Erfassen und Auslesen von betriebsrelevanten Statusinformationen oder den Neustart (Reboot) eines Systems. Durch das modulare Konzept ist das SINA Management flexibel einsetzbar. Es lässt sich – stand alone – auf einem einzelnen PC oder auch hierarchisch gestaffelt und verteilt auf mehreren Servern betreiben. Diese Modularität erlaubt eine Vielzahl von Konfigurationen und redundanten Szenarien.

Vorteile

- Zentrale Verwaltung von SINA Komponenten und Benutzern
- Getrennte Rollen für Kryptoverwaltung und Konfigurationsmanagement
- Bedarfsgerecht dimensionierbar für Netze mit unterschiedlicher Komplexität
- Statische (Offline-) oder aktiv gesteuerte (Online-) Konfiguration

Bestandteile des SINA Managements

SINA Console
Die SINA Console ist die zentrale graphische Konfigurations- und Steuerungsoberfläche (GUI) im SINA Management. Darin werden auf komfortable und übersichtliche Weise alle SINA Komponenten, Benutzer und deren Verbindungen untereinander als einzelne Objekte oder auch in Gruppen verwaltet. In der SINA Console werden die Smartcards mit allen erforderlichen Daten (insbesondere Konfigurationseinstellungen, Schlüssel, Zertifikate) beschrieben. Dabei werden u. a. PIN-Briefe und Versandinformationen generiert sowie Informationen über Ausstellungsprozess und die Gültigkeitsdauer von Schlüsseln in der Datenbank hinterlegt. Weiterhin werden in der SINA Console die Daten für das Online-Management auf den Verzeichnisdienst (LDAP-Server) geschrieben.

SINA PKI
Die sichere Authentifizierung während des Verbindungsaufbaus zweier SINA L3 Komponenten erfolgt mittels digitaler Unterschriften. Die dafür benötigten Zertifikate werden durch die SINA PKI (Public-Key-Infrastruktur) erzeugt. Grundlegende Bestandteile der SINA PKI sind eine Zertifizierungsinstanz (CA), eine Registrierungsinstanz (RA) sowie ein CMP (Certificate Management Protocol)-Server.

Verzeichnisdienst LDAP
Der LDAP-Verzeichnisdienst erlaubt die Online-Aktualisierung von Kommunikationsbeziehungen der SINA Komponenten, die Verteilung von Updates und Sperrlisten sowie die Änderung einiger kryptographischer Parameter des SINA Systems. Um die Ausfallsicherheit zu erhöhen, kann der LDAP-Server redundant ausgelegt werden.

Zeitserver (NTP)
Der NTP-Dienst ermöglicht einheitliche Systemzeiten für zugehörige SINA Komponenten und das SINA Management.

Syslog-Server
Die von SINA Komponenten generierten Logdaten werden vom Syslog-Server entgegengenommen und gespeichert.

Systemvoraussetzungen

Das SINA Management unterstützt Standardhardware mit dem Betriebssystem Red Hat Enterprise Linux (RHEL).

Betriebsüberwachung

Eine Überwachung der SINA Komponenten ist über die Einbringung von Monitoring-Informationen (Syslog, SNMP) in vorhandene Netzwerkmanagement-Systeme möglich.

BSI-Freigabe

Die einzelnen Softwareversionen des SINA Managements werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) evaluiert und für den Betrieb freigegeben.

Bezugsquellen

Behördenkunden in Deutschland können die SINA Komponenten aus dem Rahmenvertrag 5070 „Kryptiergeräte der SINA Familie“ des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Allen anderen nationalen und internationalen Kunden steht secunet gern zur Verfügung.

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

SINA Management_DE_10/20