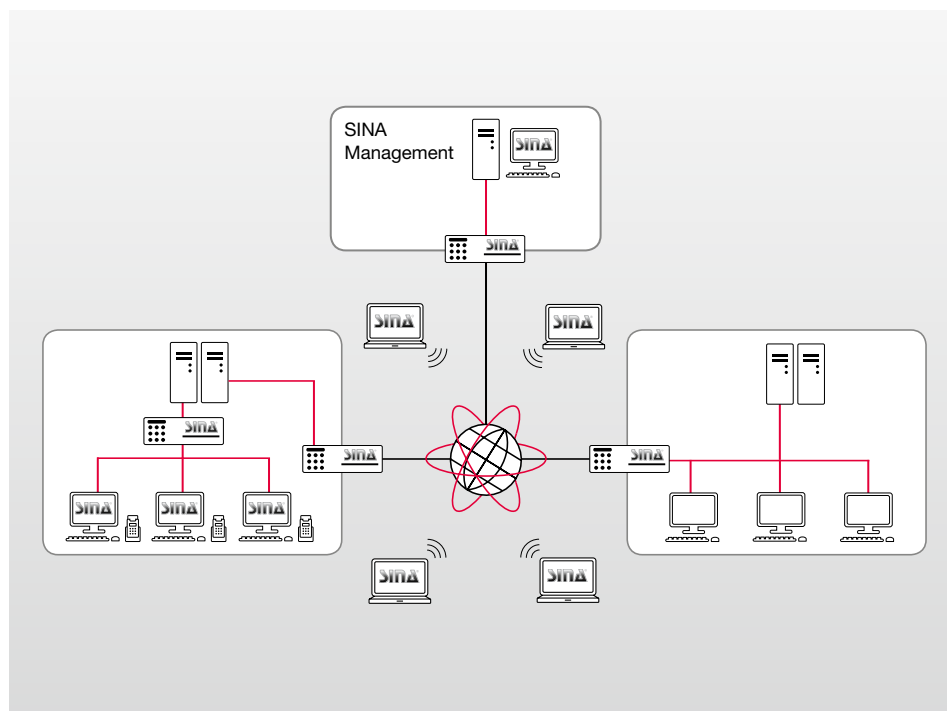


Konfiguration und Verwaltung Ihrer SINA Infrastruktur



Ihre Vorteile:

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

Das SINA Management verwaltet und konfiguriert zentral alle (in den Netzwerkschichten 3 und 2 verschlüsselnden) Komponenten der SINA Produktfamilie. Die zu schützenden Netze werden mit Hilfe des SINA Managements strukturiert aufgebaut, konfiguriert und administriert. Die graphische Benutzeroberfläche ermöglicht die einfache Konfiguration der Zugangsberechtigungen zwischen den SINA Komponenten und Netzen.

Funktionsweise des SINA Managements

Das SINA Management erfasst Konfigurationsdaten, wie z. B. Zertifikate, IP-Adresskonfiguration und Routing-Informationen und schreibt diese Daten auf ein vertrauenswürdiges und geschütztes Speichermedium (Smartcard oder USB-Token mit integrierter Smartcard). Auf den Smartcards werden die Konfigurationsdaten sicher gespeichert und stehen den SINA Komponenten zur Verfügung.

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 einzelne Sicherheitsbeziehungen
- Erzeugung von Authentifizierungsschlüsseln für SINA L2 Boxen
- Sichere Online-Updates kryptographischer Parameter
- Ausstellung und Online-Update von Signatur- und Verschlüsselungszertifikaten für SINA L3 Boxen und Benutzer
- 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 bestimmte Aktionen initiieren, u. a. das Veranlassen von Zertifikats-Updates, das Erfassen und Auslesen von betriebsrelevanten Statusinformationen oder den Neustart (Reboot) eines Systems. Die SINA Komponenten nehmen diese Aufforderungen über das Netzwerk entgegen, sofern dies durch das SINA Management konfiguriert wurde.

Durch modular aufgebaute Server und Administrationskonsolen ist das SINA Management flexibel einsetzbar. Es lässt sich – stand alone – auf einem einzelnen PC oder hierarchisch gestaffelt und verteilt auf mehreren Servern installieren und einsetzen. Diese Modularität erlaubt eine Vielzahl von Konfigurationen und redundanten Szenarien.

Bestandteile des SINA Managements

SINA PKI

Das Zertifikatsmanagement basiert auf einer Public-Key-Infrastruktur (PKI) und erzeugt Schlüsselpaare und Zertifikate beim Ausstellen der Smartcards. Mit diesen werden SINA Benutzer oder SINA Komponenten während des Verbindungsaufbaus mittels digitaler Unterschriften sicher authentifiziert. Beim Erzeugen der Smartcards werden weitere kryptographische Parameter auf die Smartcard geladen, PIN-Briefe und Versandinformationen generiert und Einträge über Ausstellungsprozess und Gültigkeitsdauer in einer Datenbank hinterlegt. Grundlegende Bestandteile des Zertifikatsmanagements sind dabei eine Zertifizierungsinstanz (CA) und eine Registrierungsinstanz (RA) sowie ein CMP (Certificate Management Protocol) -Server.

Verzeichnisdienst LDAP

Das Online-Management ermöglicht mit Hilfe eines LDAP-Verzeichnisdienstes die Kommunikationsbeziehungen der SINA Komponenten online zu aktualisieren, Updates und Sperrlisten für Notfälle zu verteilen sowie

einige kryptographische Parameter des SINA Systems zu ändern. Um die Ausfallsicherheit weiter zu erhöhen, kann der LDAP-Server auch redundant ausgelegt werden.

Zeitserver (NTP)

Der NTP-Dienst ermöglicht einheitliche Systemzeiten zugehöriger SINA Komponenten und des SINA Managements.

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) ab Version 5 und kann auf entsprechender RHEL-kompatibler Hardware betrieben werden.

Betriebsüberwachung

Eine Überwachung der SINA Systeme ist über verschiedene Integrationsmöglichkeiten der Monitoring-Informationen (Syslog, SNMP) in vorhandene Netzwerkmanagement-Systeme möglich.

BSI-Freigabe

Die einzelnen Softwareversionen des SINA Managements werden durch das BSI evaluiert und für den Betrieb freigegeben.

Bezugsquellen

Behördenkunden in Deutschland können die SINA Komponenten aus dem Rahmenvertrag BA 4867/01 des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Allen anderen nationalen und internationalen Kunden steht secunet gern zur Verfügung.

Über SINA

Im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelte secunet die Sichere Inter-Netzwerk Architektur SINA. Die Kryptosystem-Produktfamilie ermöglicht eine bedarfsgerechte, zulassungskonforme sichere Bearbeitung, Speicherung und Übertragung von Verschlusssachen (VS) sowie anderen sensiblen Daten.

Das Produktportfolio umfasst ein Management, unterschiedliche Gateways, Leitungsverchlüsseler und Clients, die seit vielen Jahren bereits bei Behörden, Streitkräften und geheimschutzbetreuten Unternehmen eingesetzt werden. Ausgewählte SINA Komponenten sind für die Verarbeitung und Übertragung von VS der Einstufungen bis einschließlich STRENG GEHEIM, NATO SECRET und SECRET UE zugelassen.

Weitere Informationen:
www.secunet.com/management

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com