UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

USP NETWORK AUTHENTICATION SYSTEM®

Technical Whitepaper

Die Sicherung des Netzwerkzugangs wird für Unternehmen mehr und mehr zur Herausforderung. Vor allem in grossen, weitläufigen Netzwerken ist mit konventionellen Mitteln nicht mehr kontrollierbar, welche Endgeräte ans Netz angeschlossen werden. Aber auch in kleinen Netzwerken tritt diese Thematik immer stärker in den Vordergrund. Die daraus resultierenden Gefahren liegen auf der Hand: Aufgrund des unkontrollierten Zugangs zum Netzwerk erlangen Besucher wie z.B. externe Berater sehr leicht Zugriff auf vertrauliche Daten. Kontaminierte Geräte verbreiten Viren, Würmer und andere Schadsoftware fast ungehindert. Der Einsatz von privaten Geräten erhöht die Hardwarevielfalt und die Fehleranfälligkeit und die Kosten des IT-Supports.

Version 1.2

United Security Providers AG
www.united-security-providers.ch
info@united-security-providers.ch

Headquarter Stauffacherstrasse 65/15, CH-3014 Bern
Baslerpark Mürtschenstrasse 27, CH-8048 Zürich

Phone +41 31 959 02 02

DAS USP NETWORK AUTHENTICATION SYSTEM®

Das USP Network Authentication System® (USP NAS) von United Security Providers schützt zuverlässig vor diesen Gefahren. Es erkennt und identifiziert alle Geräte, die ans Firmennetzwerk angeschlossen werden und regelt deren Zugang zum Netzwerk. Unerlaubte Zugriffe werden dadurch verhindert. Firmeneigene Geräte erhalten Zugriff auf genau die Ressourcen, für die sie tatsächlich befugt sind. Abhängig von der konfigurierten Policy reagiert das System auf Zugriffsverletzungen nicht autorisierter Geräte mit einer Vielzahl von Möglichkeiten (z.B. Verschieben des Geräts in eine Quarantäne-Zone, Blockierung des Zugangs, Auslösen eines Alarms).

USP NAS bietet einen sofortigen und vollständigen Überblick über das Netzwerk und regelt und protokolliert die Zugriffe aller anschliessbaren Endgeräte.

Der Einsatz des USP NAS schafft folgenden Nutzen:

- Der Zugriff und die Integrität der Endgeräte können kontrolliert und geregelt werden.
- Der Zugang zum Netzwerk wird durch ein Regelwerk gesteuert, das flexibel an die Bedürfnisse angepasst werden kann.
- Es kann sich jederzeit ein aktuelles Bild über die am Netzwerk aktiven Endgeräte verschafft werden (Standort, Anschluss, IP-Adresse, etc.)
- Die Konfiguration der Policy erfolgt einfach und intuitiv. So kann zum Beispiel ein zuverlässiger firmenweiter Guest Network Service mit wenigen Mausklicks eingerichtet werden.
- Die vom System ermittelten Informationen liefern einen wertvollen Beitrag für ein effektives Service Management und können unter anderem zur Optimierung der Qualität der Inventardatenbank oder zur Unterstützung der Kosten- und Leistungsverrechnung verwendet werden.
- Compliance Informationen von Drittsystemen können für die Policy-Zuweisung genutzt werden.
- Die Lösung funktioniert agentenlos und herstellerunabhängig.
- Die Lösung unterstützt den IEEE 802.1X Standard.
- Die Lösung kann innert Stunden einfach in Betrieb genommen werden und liefert dank des integrierten Reportings bereits ab dem ersten Tag wertvolle Informationen.

© United Security Providers AG

DIE LÖSUNG

Das USP Network Authentication System® ist eine zentrale, modular aufgebaute out-of-band Network Access Control Lösung (NAC), die agentless und herstellerunabhängig, auf Basis einer regelbasierten Policy, das Access Control Enforcement umsetzt. Ein rollenbasiertes Web GUI in mehreren Sprachen, umfangreiches integriertes Reporting und die flexible Anbindung von Inventarsystemen rundet die stabile und praxiserprobte Lösung ab.

Das USP Network Authentication System® (USP NAS) verhindert nicht nur unerlaubte Zugriffe auf das Firmennetz, sondern punktet mit zusätzlichen Funktionen.

Das USP Network Authentication System® unterstützt out-of-the-box die gängigen Hersteller von Netzwerkkomponenten, beispielsweise Cisco, Alcatel, HP/Aruba, H3C, Extreme, Ubiquiti, usw. Da das USP Network Authentication System® agentless funktioniert, stellt das System grundsätzlich keine spezifischen Anforderungen an die Endgeräte.

Erhältlich ist die Lösung als Hardware- und als virtuelle Appliance (z.B. VMware ESX / Microsoft Hyper-V). Die USP Network Authentication System® Hardware-Appliance basiert auf einer Standard Rackserver Architektur, die mit redundanten Harddisks und redundanten Powersupplies ausgestattet ist. Diese Architektur ermöglicht einen robusten Betrieb, denn die anfälligsten Bauteile können zur Laufzeit ausgewechselt werden. Die Appliance ist hochgradig skalierbar. Mit der Standardausprägung der Hardware überwacht eine Appliance heute bei einigen unserer Kunden mehr als 60'000 Endgeräte und über 10'000 Switches und Router. Wahlweise kann die Appliance redundant hochverfügbar betrieben werden.

Standardschnittstellen für die externe Überwachung der Appliance (SNMP, syslog, SMTP) sowie integrierte Funktionen für automatisierten Backup, ein allfälliger Restore und periodische Softwareupdates ermöglichen eine einfache Integration in die vorhandene Betriebsinfrastruktur und erleichtern den täglichen Betrieb.

Das USP NAS stellt sicher, dass der Zugang auf das Netz überwacht und geschützt ist. Gleichzeitig verhindert es, dass unbekannte Endgeräte Zugriff auf das Netz haben. Ferner gewinnt der Kunde mit dem USP NAS eine laufend aktualisierte Übersicht über die angeschlossenen und autorisierten Geräte.

Das USP NAS zeichnet sich durch eine schnelle Integration in bestehende Infrastrukturen aus und ist damit in der Lage, ein Unternehmensnetzwerk rasch und zuverlässig abzusichern.

© United Security Providers AG

KONTROLLIERTER ZUGANG ZUM NETZWERK

Das USP Network Authentication System® (USP NAS) von United Security Providers verhindert nicht nur unerlaubte Zugriffe auf das Firmennetz. Es leistet weit mehr.

Nur bekannte bzw. erfolgreich authentisierte Geräte erhalten Zugang zum produktiven Netzwerk. Unbekannte Geräte oder solche, die sich mittels 802.1X / EAP nicht erfolgreich authentisieren können, werden gesperrt. Je nach konfiguriertem Modus erfolgt die Sperrung per Port-Shutdown oder durch Setzen eines Quarantäne VLANs. Diese Regeln können für spezifische Gruppen von Netzgeräten sowie Endgeräten separat konfiguriert werden. Für externen Mitarbeitern oder Gäste können Geräte temporär erfasst werden; nach einer definierten Zeit werden diese wieder automatisch aus dem Inventar entfernt.

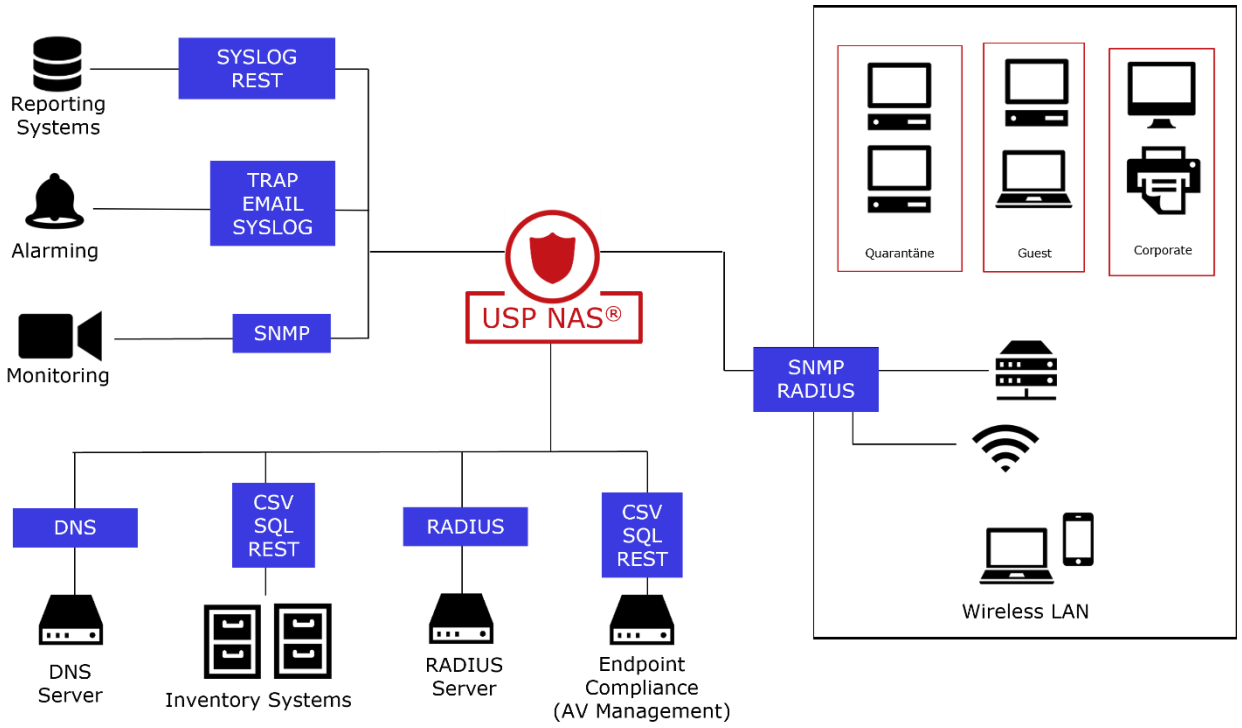

Abbildung 1: Übersicht Funktionsweise USP NAS

AUTHENTISIERUNG DER GERÄTE

Die Authentisierung der Geräte kann mittels IEEE 802.1X oder alternativ über die MAC-Adressen erfolgen, wobei die beiden Ansätze flexibel miteinander kombinierbar sind.

- 802.1X: Die Endgeräte schalten sich den Zugang zum Netzwerk mittels IEEE 802.1X frei, die Authentisierung erfolgt im Normalfall durch ein digitales Zertifikat (EAP-TLS).
- Radius MAC Authentisierung: Der Switch stellt selbständig auf MAC basierte Authentisierung um, wenn er ein Endgerät detektiert, das kein 802.1X unterstützt. Die Authentisierung erfolgt anschliessend über das standardisierte Radius-Protokoll. Das USP NAS fällt den Entscheid anhand der MAC-Adresse des Endgeräts.
- SNMP MAC Authentisierung: Als Alternative zu RADIUS / 802.1X können Endgeräte auch mittels SNMP detektiert, identifiziert und authentisiert werden. Dies erlaubt einen ausfallsicheren Betrieb, mit minimalen Anforderungen an die Netzwerkinfrastruktur.
- Hybrider Betrieb mit SNMP und RADIUS Authentisierung: 802.1X geschützte Ports können flexibel zusammen mit der SNMP / MAC Authentisierung als Grundschutz kombiniert werden. Es ist so auch problemlos möglich 802.1X schrittweise, nur in gewissen Bereichen des Netzwerks einzuführen.

Die Möglichkeit MAC und 802.1X Authentisierung in dem sogenannten Hybridbetrieb gleichzeitig einzusetzen, ist ein entscheidender Vorteil der Lösung. Dies ermöglicht grosse Flexibilität im Einsatz von 802.1X und erlaubt die sukzessive Einführung des 802.1X Standards. Der herstellerunabhängige MAC Authentisierungs-Mechanismus stellt zudem den Anschluss von Legacy Geräten an 802.1X Ports sicher.

Unabhängig vom verwendeten Mechanismus ist sichergestellt, dass die Informationen über das neu am Netzwerk angeschlossene Endgerät in die Datenbank des Systems fliessen, so dass es jederzeit möglich ist, über die im Netz aktiven Endgeräte Auskunft zu geben.

ÜBERSICHT ÜBER DIE ENDGERÄTE

USP NAS verwendet verschiedene Informationsquellen, um ein möglichst vollständiges Bild über die Endgeräte am Netzwerk liefern zu können:

- Regelmässige Scans von Switches und Routern mittels SNMP zur Ermittlung der Portkonfiguration und der verwendeten IP-Adresse.
- Regelmässige Importe aus dem DNS mittels Zone-Transfer, sodass zu den IP-Adressen auch passende DNS-Namen angegeben werden können.
- Interpretation des 802.1X Authentisierungsdialogs mit anschliessender Verknüpfung dieser Informationen mit den Informationen aus den SNMP-Scans.
- Mittels Device Profiling können zusätzliche Geräteinformationen, zum Beispiel das Betriebssystem, angezeigt werden.

Alle Informationen werden in der USP NAS Datenbank verwaltet und können sowohl für Policy Entscheidungen wie auch für Auswertungen verwendet werden.

© United Security Providers AG

POLICY-ENTSCHEIDUNGEN

Die über ein Endgerät ermittelten Informationen werden durch ein flexibel einstellbares Regelwerk ausgewertet, um anschliessend entscheiden zu können, ob das Endgerät am Netzwerk kommunizieren darf oder nicht.

Abhängig vom Zugangsentscheid können aufgrund der definierten Policy, unterschiedliche Massnahmen erfolgen:

- Verschieben des Switch-Ports oder der WLAN-Terminierung in ein anderes VLAN (z.B. verschiedene produktive VLANs, Quarantäne-VLANs oder Gäste-VLANs).
- Automatisches Sperren des Zugangs respektive Nicht-Freischalten im Fall von 802.1X.
- Semi-automatisches Sperren des Zugangs (die Sperrung erfolgt erst nach Bestätigung durch einen Network-Operator).
- Loggen der nicht-konformen Geräte, die anschliessend mittels Reports ausgewertet werden können.
- Auslösen einer Meldung über E-Mail, Syslog oder SNMP.
- Policy-Enforcement aufgrund von Geräteprofilen.

Das USP NAS Regelwerk erlaubt es, diese Massnahmen selektiv einzusetzen. Die zur Anwendung gelangende Massnahme kann z.B. vom Typ des Geräts, von Zertifikats-Attributen, von seinem Standort im Netzwerk oder seiner Zugehörigkeit zu einem Mandanten abhängig gemacht werden.

Die Regeln greifen wahlweise unternehmensweit, eingeschränkt auf Netzwerkbereiche, auf eine Anzahl Switches / Wireless Access Controller oder gar auf beliebige Gruppen einzelner Access Ports. Dadurch kann auf einfache Weise eine firmenweite Policy festgelegt werden, die – dort wo es notwendig ist – beliebig verfeinert werden kann. Mit Regeleditor und Policy Manager stehen dem Benutzer auf dem Web GUI zwei effiziente und übersichtliche Werkzeuge für die Verwaltung des Regelwerks zur Verfügung.

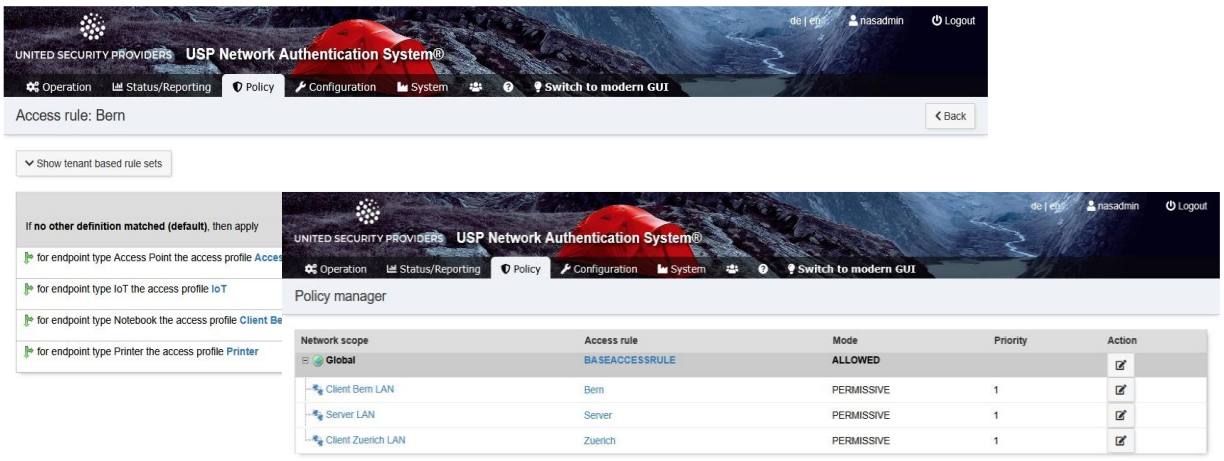

Abbildung 2: Regeleditor und Policy Manager

DYNAMISCHES VLAN MANAGEMENT

Das dynamische VLAN-Management ermöglicht eine äusserst flexible Steuerung des Zugangs beim Anschluss der Endgeräte ans Netzwerk. Abhängig von verschiedenen Kriterien werden die Endgeräte in die gewünschte VLAN-Zone verschoben:

Standortspezifischer Zugang

Für verschiedene Teile des Netzwerks können unterschiedliche VLAN für Sperrung, Quarantäne, Gastzugang und den produktiven Zugang konfiguriert werden. Die Netzwerkteile können dabei beliebig feingranular definiert sein (falls notwendig bis hin zu einzelnen LAN-Ports).

Gerätespezifischer Zugang

Es ist möglich, den Zugang für bestimmte Typen von Geräten spezifisch zu regeln. So können zum Beispiel Drucker oder spezielle Hardware in andere produktive VLAN gesetzt werden als die typischen Endgeräte der Benutzer (Laptops oder PCs). Falls notwendig, kann für jedes einzelne Gerät festgelegt werden, in welches produktive VLAN es gesetzt werden soll).

Mandantenspezifischer Zugang

Der Einbezug von Mandanteninformationen (der Endgeräte und der Netzwerkteile) ermöglichen eine unterschiedliche Regelung des Zugangs im Heim-Netz und in fremden Netzwerkteilen. Dies erlaubt es Mitarbeitern auf Dienstreise eingeschränkte Zugangsrechte auf Zweigniederlassungen zu gewähren. Die Endgeräte werden dazu im eigenen Teil des Netzwerks zum Beispiel ins Home VLAN (das entsprechende produktive VLAN) geschoben, in anderen Netzwerkteilen hingegen ins Gast VLAN.

DEVICE PROFILING

Das Device-Profiling erstellt einen Fingerprint aller, mit den am Netzwerk verbundener, Geräte: Geräteart, Herstellername, Betriebssystem, Version. Es stellt umfassende Informationen über die am Netzwerk angeschlossenen Endgeräte zur Verfügung und klassiert diese als Grundlage für Reports und Statistiken.

Automatische Inventarisierung

Basierend auf einer Device Profile White-List können z.B. None-PC Geräte wie Drucker, Überwachungskameras oder IP-Phones automatisch inventarisiert und einer Gerätekategorie zugewiesen werden.

Effizienter Inventaraufbau

Device Profiling ermöglicht einen effizienten Inventaraufbau, indem alle Geräte, insbesondere auch die unbekannten/nicht inventarisierten, erfasst werden.

Intrusion Detection und Prevention

Durch kontinuierliches Profiling der angeschlossenen Endgeräte können Angriffe z.B. MAC Spoofing erkannt und der Zugang für diese Geräte gesperrt werden.

© United Security Providers AG

RADIUS SERVER

Kleinere und mittlere Netzwerke verfügen oft über keine Radiusserver Infrastruktur. Deshalb bietet USP NAS diese Funktion bei Bedarf als Modul an. Das Radiusserver Modul unterstützt zertifikatsbasierte Authentisierungen (EAP-TLS). Mit dem Online Certificate Status Protocol (OCSP) kann die Gültigkeit der Zertifikate auf einer Public Key Infrastructure (PKI) überprüft werden.

ENDPOINT COMPLIANCE

Zur Bestimmung des Zugangs zum Netzwerk wird optional der Konfigurationszustand des Endgerätes berücksichtigt (Endpoint Compliance). So wird sichergestellt, dass nur Geräte ans Netz gelangen, die über eine aktuelle und gültige Konfiguration verfügen. So kann zum Beispiel der Einsatz von Virenscannern erzwungen oder die Aktualität der Betriebssystem-Patches sichergestellt werden.

Health-Profil

Mittels Health-Profilen kann ein Soll-Gesundheitszustand für Endgeräte definiert werden. Für den Gesundheitszustand kommen Informationen bezüglich Virenschutz, Anti-Spyware, Firewall und OS-Informationen zu Einsatz. Ein Health-Profil besteht aus mehreren Policies, die erfüllt sein müssen, damit der Zustand eines Gerätes als „gesund" eingestuft wird. Health-Profile definieren auch, welche Aktionen ausgeführt werden, wenn Abweichungen vom Soll-Zustand vorliegen.

Im Health-Profil werden zeitliche Limits definiert, damit klar ist, ab wann eine Abweichung vom Soll-Zustand einen Alarm oder eine bestimmte Aktion – z.B. das Sperren des Gerätes – auslöst. In einem System können unterschiedliche Health-Profile verwendet werden, die einzelnen Geräten oder Gruppen von Geräten zugewiesen werden. Ebenso ist es möglich, auf verschiedenen Netzwerkteilen unterschiedliche Soll–Profile zu verwenden.

Generische Health-Import Schnittstelle

Nebst dem integrierten Scanner besteht die Möglichkeit die Health- Information der Endgeräte, über die Health-Importschnittstelle aus Fremdsystemen, mittels CSV-Dateien zu importieren. Mit der generischen Health-Import Schnittstelle ist es ebenfalls möglich, bereits bestehende Health-Überwachungssysteme als Source für den Gesundheitszustand der Endgeräte zu verwenden.

© United Security Providers AG

MANDANTENFÄHIGKEIT

Das System erlaubt die Verteilung der Verwaltung und des Betriebs verschiedener Systemteile auf unterschiedliche Benutzerkreise. Dazu werden die verschiedenen Teile des Netzwerkes und optional die registrierten Endgeräte frei definierbaren Mandanten zugeordnet. Für jeden Benutzer des USP Network Authentication System® wird festgelegt, für welche Mandanten er berechtigt ist. Die dem Benutzer zugesprochenen Rechte kann er nur auf den ihm zugewiesenen Mandanten nutzen.

Die Benutzer können über das Web GUI genau diejenigen Netzwerkteile des Systems einsehen, für die sie berechtigt sind. Dies ermöglicht die Einschränkung der Informationen nach dem Prinzip „Need-to-Know", sprich die Benutzer sehen nur die Informationen, die sie für ihre Tätigkeit benötigen.

Die Benutzer können auch nur auf diejenigen Teile des Netzwerkes Einfluss nehmen, für die sie berechtigt sind. Sie können über das Web GUI nur Geräte innerhalb der für sie freigegebenen Mandanten freischalten oder temporär registrieren. Dies ermöglicht die Verteilung der betrieblichen Rollen in grösseren Unternehmen.

USER INTERFACE

Für die Benutzeroberfläche kommt ein Web GUI, mit rollenbasiertem Berechtigungsmodell, zum Einsatz. Sowohl Web GUI als auch alle Reports und die Benutzerdokumentation stehen in mehreren Sprachen zur Verfügung.

Abhängig von der Rolle des Benutzers stehen unterschiedlich viele Funktionen zur Verfügung:

- Helpdesk Rolle: Kann die Liste der nicht-konformen Endgeräte einsehen und den gesperrten oder sich in Quarantäne befindenden Endgeräten den Netzzugang freischalten.
- Network-Support Rolle: Kann zusätzlich einfache Einstellungen am Regelwerk sowie Anpassungen an der Liste der zu überwachenden Switches und Router vornehmen.
- Administrator Rolle: Kann zusätzlich sämtliche Konfigurationseinstellungen und das USP NAS Regelwerk anpassen, Benutzer erfassen, Benutzer löschen und Rollen zuweisen.
- Monitoring Rolle: Nur für Statusabfrage (USP NAS Health Check) der USP NAS Prozesse Trap-Handling und USP NAS Dienst.
- Reporting Rolle: Generieren und Einsehen von Reports und Logfiles für Endgeräte, Netzwerkgeräte und betriebliche Auswertungen wie User Report, MAC-Tracker etc.

Bei Anpassungen am Regelwerk werden dem Benutzer die Auswirkungen seiner Änderung in Form einer Impact Analyse dargestellt, bevor diese nach Bestätigung durch den Benutzer effektiv in Kraft gesetzt werden. Auf diese Weise lassen sich Betriebsstörungen durch Fehlmanipulationen weitgehend vermeiden.

© United Security Providers AG

REPORTING

Das USP NAS historisiert alle im überwachten Netzwerk auftretenden Ereignisse. Die vorhandenen Daten erlauben daher eine transparente Sicht auf das Netzwerk, sowohl für gegenwärtige und als auch vergangene Ereignisse. Eine integrierte Reporting Engine erzeugt parametrisierbare Berichte und Statistiken, die die IT-Mitarbeiter unter anderem bei der Überwachung oder Auditierung der Netzwerkzugriffe, der angeschlossenen Geräte oder der Netzwerkkomponenten unterstützt. Die Berichte können durch das USP NAS, über das Scheduled Reporting, bei Bedarf auch zeitgesteuert, d.h. regelmässig zu einem fixen Zeitpunkt, mit einer vordefinierten Parametrisierung, generiert werden.

Die Berichte ermöglichen einerseits statistische Auswertungen, anderseits erlauben sie die Auswertung der Ereignisse einzelner Geräte oder Netzwerkkomponenten. Die Berichte können in verschiedenen Standardformaten dargestellt werden.

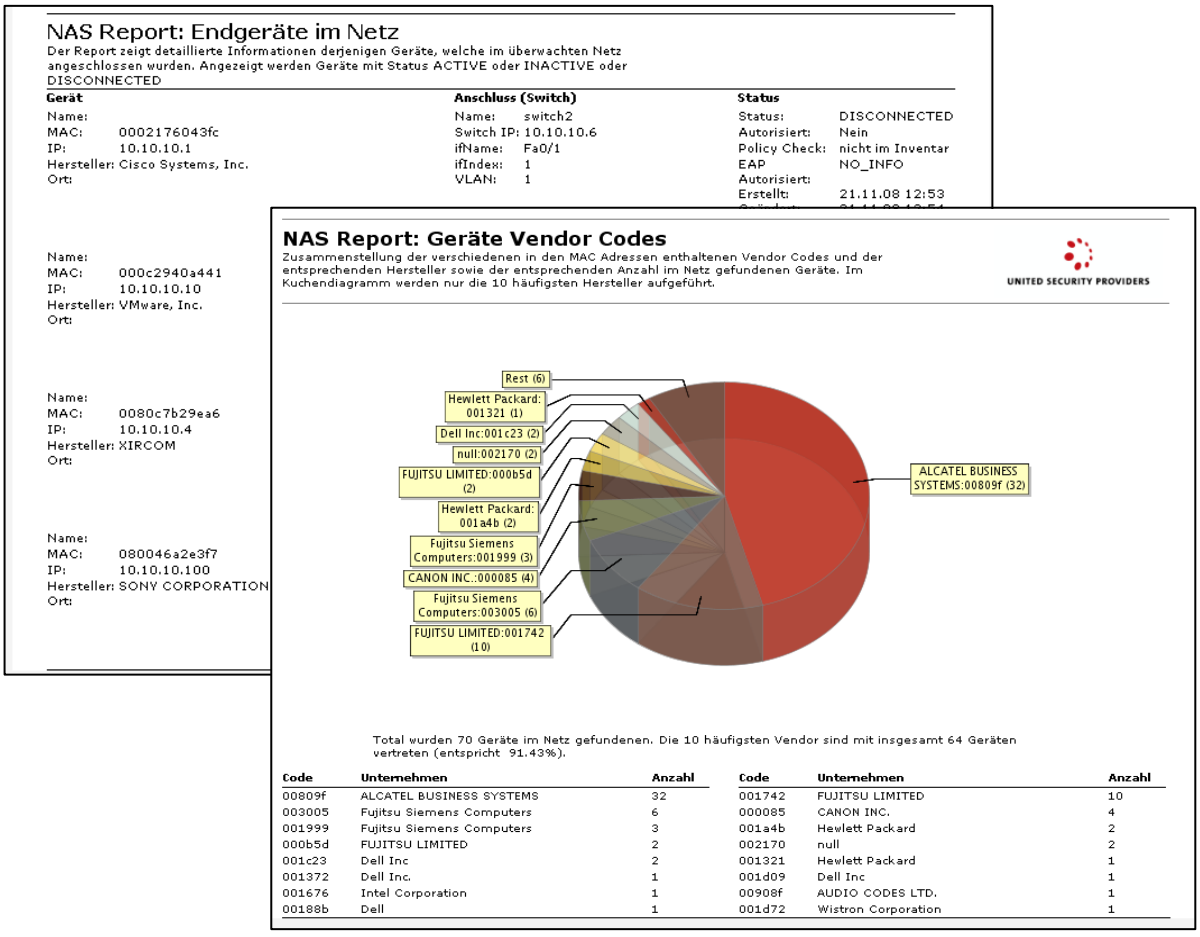

Abbildung 3: Beispielreports

UNITED SECURITY PROVIDERS

ALARMING & MONITORING

Sämtliche Ereignisse im Netzwerk und im USP Network Authentication System® werden in der internen Datenbank gespeichert und können optional über drei verschiedene Arten (E-Mail, Syslog, SNMP) weitergeleitet bzw. alarmiert werden. Diese Funktionalität ermöglicht eine einfache Integration in bestehende Überwachungssysteme.

Durch die flexibel konfigurierbare Weiterleitung der verschiedenen Meldungen kann z.B. ein Administrator über die Sperrung eines Clients in Kenntnis gesetzt werden, bevor der betroffene Mitarbeiter zum Telefon gegriffen hat. Auch kann im RZ-Bereich mittels Alarming und Permissiv- Modus über den Neuanschluss eines unbekannten Gerätes informiert werden.

Das integrierte Monitoring des USP Network Authentication System® ermöglicht die einfache Überwachung der Appliance inklusive Hardware, Betriebssystem und Applikation. Ebenso werden die konfigurierten Umsysteme überwacht. Lässt sich zum Beispiel ein Switch über eine längere Zeit nicht über SNMP ansprechen, wird ein Alarm ausgelöst.

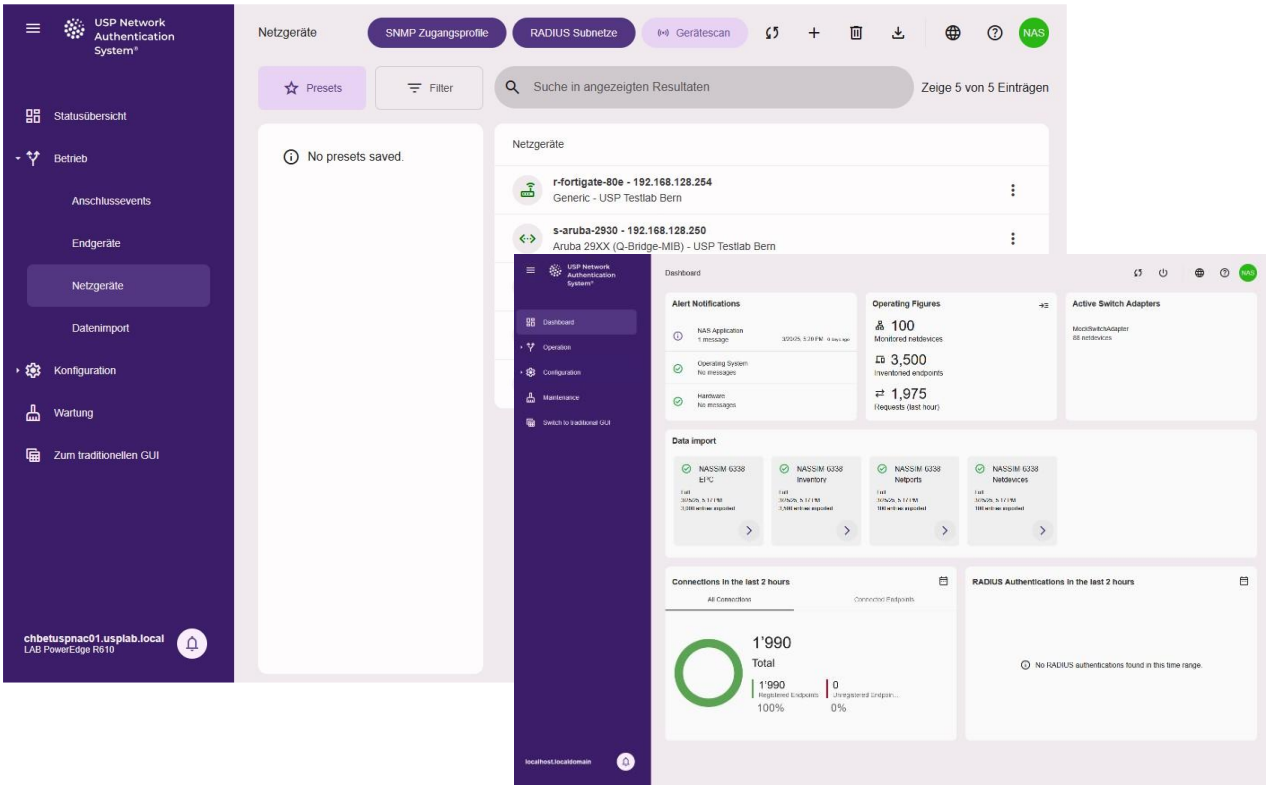

Abbildung 4: Dashboard & Netdevice Übersicht

REDUNDANZ

Für einen redundanten Betrieb kann eine MASTER Appliance mit einer oder mehreren Appliances ergänzt werden, die in einem AUTHENTICATOR Modus betrieben werden. Im AUTHENTICATOR Modus holt sich die Instanz selbständig die aktuelle Konfiguration von der MASTER Appliance und steht jederzeit für RADIUS Authentisierungs-Anfragen bereit. Mit dieser Architektur wird eine lose Kopplung und damit ein stabiler und maximal ausfallsicherer Betrieb für die RADIUS Authentisierungen ermöglicht.

VERTEILTE ARCHITEKTUR

In gewissen Fällen kann es sinnvoll sein, vom zentralen Ansatz abzuweichen. Dies ist unter anderem dann der Fall, wenn die verschiedenen Standorte untereinander mit unzuverlässigen WAN-Links verbunden sind und gleichzeitig aber eine hohe Verfügbarkeit des gesamten Systems verlangt ist.

In solchen Fällen ist es möglich, USP Network Authentication System® auch im Rahmen einer verteilten Architektur zu betreiben und so die Überwachung des Netzwerks auf mehrere Appliances zu verteilen. Die Administration sowie das Reporting kann in einem solchen Setup dennoch zentral erfolgen.

Hierzu wird analog der Redundanz Architektur der MASTER / AUTHENTICATOR Ansatz eingesetzt, wobei an einem Standort die Instanz im MASTER Modus betrieben wird und an den übrigen Standorten beliebig viele Instanzen im AUTHENTICATOR Modus betriebe werden.

SCHNITTSTELLEN

Bereits vorhandene Netzwerkmanagement- und Inventarsysteme können mit geringem Aufwand integriert werden. Auf diese Weise müssen beispielsweise die zu überwachenden Switches und Router nicht noch in einem weiteren System gepflegt werden, wenn die Daten bereits in einem NMS geführt werden.

Das USP NAS stellt eine standardisierte Import-Schnittstelle zur Verfügung, die auf der Übertragung von Flat-Files von den Quellsystemen zum USP NAS Server basiert. Die Daten können zu einem beliebigen Zeitpunkt übertragen und anschliessend zeitnah von USP NAS geladen werden. Falls keine Inventare bestehen, können die erforderlichen Daten der Endgeräte und Netzwerkkomponenten im USP NAS gespeichert und über die Web GUI gepflegt werden.

Über eine Export-Schnittstelle können sowohl Inventar- als auch Betriebsdaten in Form von kommagetrennten Textdateien (CSV) exportiert werden. Dadurch kann z.B. mit aktuellen Daten aus dem Netzwerk ein Inventar aufgebaut und betrieblich relevante Daten können in einem Drittsystem weiterbearbeitet oder aufbereitet werden. In Kombination mit dem Scheduled Reporting wird es sogar möglich, Inventardaten zwischen dem USP NAS und einem Netzwerkmanagement- oder Inventarsystem automatisch abzugleichen.

TECHNISCHE INFORMATIONEN

Kommunikation mit der Netzwerk- Infrastruktur

- SNMP v1, v2c oder v3
- SNMP-Traps
- SNMP MIB-II (IP-MIB, IF-MIB, Bridge- MIB)
- SNMP Q-Bridge-MIB oder vendorspezifische MIBs für VLAN-Informationen
- IEEE 802.1X
- IEEE 802.1Q VLAN
- Dynamic VLAN Assignment
- DNS Zone Transfer (RFC 1995)

IEEE 802.1X Support

- IEEE 802.1X RADIUS (RFC 3580)
- EAP (RFC 3748, RFC 2716)
- RADIUS Proxy Support
- Interner RADIUS Server

User-Interface

- HTTPS, TLS (RFC 4346)
- Web-GUI mit rollenbasiertem Berechtigungsmodell
- Vordefinierte Rollen: Helpdesk, Support, Admin, Monitoring, Reporting
- Unterstütze Sprachen: Deutsch, Englisch

Management-Interface

- Management Web-GUI (HTTPS)
- SSHv2
- Zentrale Konfigurationsverwaltung in Web-GUI integriert

Performance und Verfügbarkeit

- Gespiegelte Datenhaltung in geografisch entfernten Standorten
- Multi-Threaded-Architektur
- Ein zentrales System kann problemlos mehrere tausend Switches/Routers und mehrere zehntausend Endgeräte überwachen.

Logging, Monitoring und Alerting

- Integrierte Monitoring-Lösung für die Überwachung der Appliance Hardware, des Betriebssystems und der Applikationsdienste. Alert-Handling und grafische Darstellung der Systemressourcen und -dienste.
- Alle wichtigen Ereignisse werden im Log für die Nachvollziehbarkeit festgehalten.
- Weiterleitung von beliebigen Typen von Logmeldungen und Alerts wahlweise mittels Syslog, SNMP-Trap und/oder E-Mail.
- Event-Scripting mit beliebig definierbaren Aktionen (z.B. Versenden von E-Mails/SMS oder Eröffnen eines Trouble-Tickets in einem Ticketingsystem).

Schnittstellen für den Datenaustausch

- Import-Schnittstelle mit Support für mehrere unabhängige Quellsysteme
- Import von CSV-Dateien via SFTP
- Export von Excel/CSV-Dateien via Web GUI
- REST API

Reporting

- In das Web GUI integrierte Reporting-Engine
- Scheduled Reporting (E-Mail / SFTP)
- Output Format: HTML, PDF oder CSV
- Möglichkeit zur Anbindung von Reporting-Tools wie z.B. Business Objects, Crystal Reports etc.

Hardware Appliance

- Standard Dell-Rackserver (1U / einfache Bauhöhe)
- Intel Xeon Quad Core CPU, 16GB RAM
- 2 Hotplug 2TB SAS Harddisks RAID 1
- 2 Hotplug-Netzteile
- Integrated Dell Remote Access Controller (iDRAC) für out-of-band Management (LOM)

Virtual Appliance

- VMware ESX / Microsoft Hyper-V / Nutanix / Proxmox / KVM-Qemu / Oracle VirtualBox / …
- Mindestens 2 CPU-Cores
- Mindestens 4 GB RAM
- 60-320 GB Harddiskplatz (abhängig von der Anzahl Endgeräte)

© United Security Providers AG