Alcatel·Lucent Enterprise

NETZWERK TRIFFT CYBERSECURITY: SICHERE UND MODERNE NETZWERKE UMSETZEN

BENJAMIN EGGERSTEDT (ALCATEL-LUCENT ENTERPRISE)

ALCATEL-LUCENT ENTERPRISE
DOK FORUM 2023

VORSTELLUNG

- Benjamin Eggerstedt
- Senior Director System Engineering Digital Age Network EMEA
- Leiter eines 30-köpfigen Teams verteilt über EMEA
- benjamin.eggerstedt@al-enterprise.com
- +49 7154 803 5302

Rainbow™

… oder über Rainbow

Alcatel·Lucent Enterprise

WAS SEHEN WIR HIER?

FOKUS AUF SICHERHEIT

DAS NETZWERK ALS STARKER PARTNER DER CYBERSECURITY

Alcatel·Lucent Enterprise

SICHERHEIT IST EIN PROZESS: BEREITS EIN FEHLER KANN ERHEBLICHE FOLGEN HABEN

Alcatel·Lucent
Enterprise

CYBERSICHERHEIT IST EIN PROZESS

Das Netzwerk ist ein wichtiger Teil davon

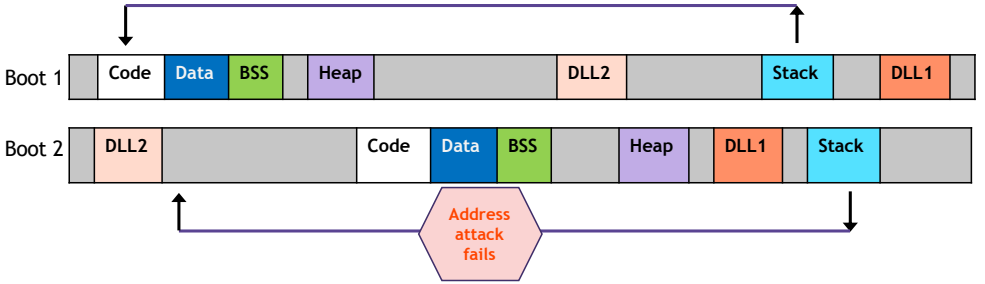
- ✓ Cybersecurity ist ein komplexer Prozess
- ✓ Nur eine Firewall reicht nicht
- ✓ Hinzufügen von Sicherheitsebenen reduziert das Risiko

Alcatel·Lucent Enterprise

ABSICHERUNG DES BETRIEBSSYSTEMS

ALE sicherer, diversifizierter Code auf OmniSwitches

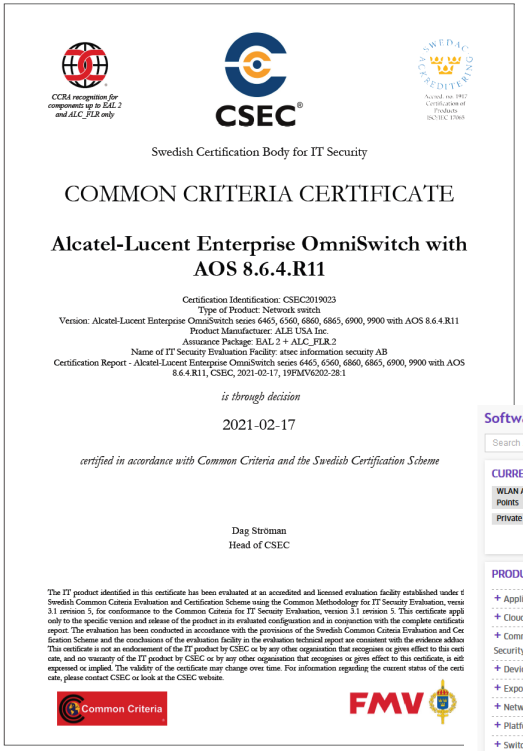
- ✓ Quellcode: Unabhängige Verifizierung & Validierung
  - Quellcode-Analyse, White-Box- und Black-Box-Tests, Suche nach Sicherheitslücken in externen Schnittstellen
- Software Diversifizierung um gleiches Verhalten von Switches auf Angriffe zu verhindern:
  - Address Space Layout Randomization (ASLR). Jeder Switch-Boot generiert ein eigenes Speicherlayout



ALE sicherer, diversifizierter Code ermöglicht eine hohe Sicherheit auf Netzwerkkomponentenlevel

Alcatel·Lucent Enterprise

ALE SICHERHEITSZERTIFIZIERUNGEN



CCRA recognition for components up to EAL 2 and ALC_FLR only

CSEC

Swedish Certification Body for IT Security

COMMON CRITERIA CERTIFICATE

Alcatel-Lucent Enterprise OmniSwitch with AOS 8.6.4.R11

Certification Identification: CSEC2019023
Type of Product: Network switch
Version: Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11
Product Manufacturer: ALE USA Inc.
Assurance Package: EAL 2 + ALC_FLR.2
Name of IT Security Evaluation Facility: atsec information security AB
Certification Report - Alcatel-Lucent Enterprise OmniSwitch series 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.6.4.R11, CSEC, 2021-02-17, 19FMV6202-28:1

is through decision

2021-02-17

certified in accordance with Common Criteria and the Swedish Certification Scheme

Dag Ströman
Head of CSEC

The IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility established under t Swedish Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, versio 3.1 revision 5, for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5. This certificate appli only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certificatio report. The evaluation has been conducted in accordance with the provisions of the Swedish Common Criteria Evaluation and Cer fication Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduc This certificate is not an endorsement of the IT product by CSEC or by any other organisation that recognises or gives effect to this certi cate, and no warranty of the IT product by CSEC or by any other organisation that recognises or gives effect to this certificate, is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certi cate, please contact CSEC or look at the CSEC website.

Common Criteria

FMV

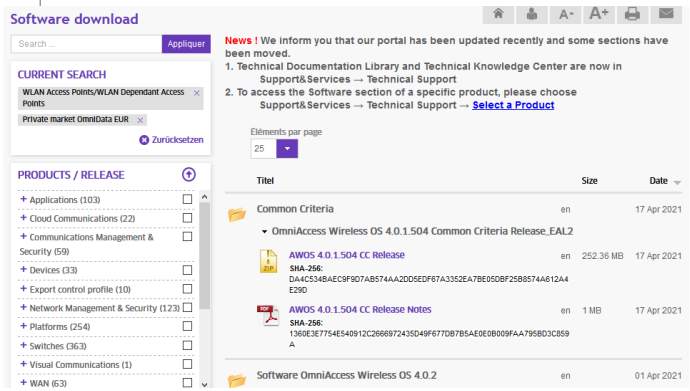
EAL2 Common Criteria CERTIFIED

NDcPP Common Criteria CERTIFIED

DEFENSE INFORMATION SYSTEMS AGENCY — JOINT INTEROPERABILITY TEST COMMAND

JITC Certified

We also maintain **certifications for :**
NDcPP (Network Device collaborative Protection Profile)
FIPS140-2 (a U.S. government computer security standard used to approve cryptographic modules)
JTIC (US Department of Defense interoperability certification)
Our Omniswitches referencing in the **list of NATO's approved equipment's.**

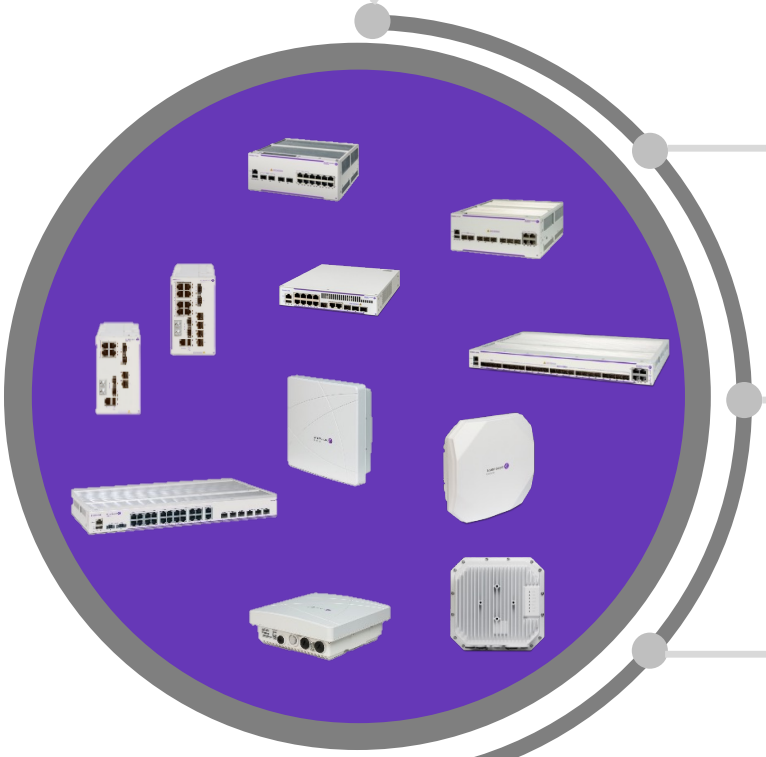


FIPS VALIDATED 140-2

Die aktuelle AOS/AWOS-Version ist im Zertifikat und im ALE MyPortal ersichtlich

Alcatel·Lucent Enterprise

HARDWAREHÄRTUNG



Industrieumgebung

IEC

Eisenbahn

EN50121-4

EN50155

Erweiterter Temp.-Bereich

Militär

NATO OTAN

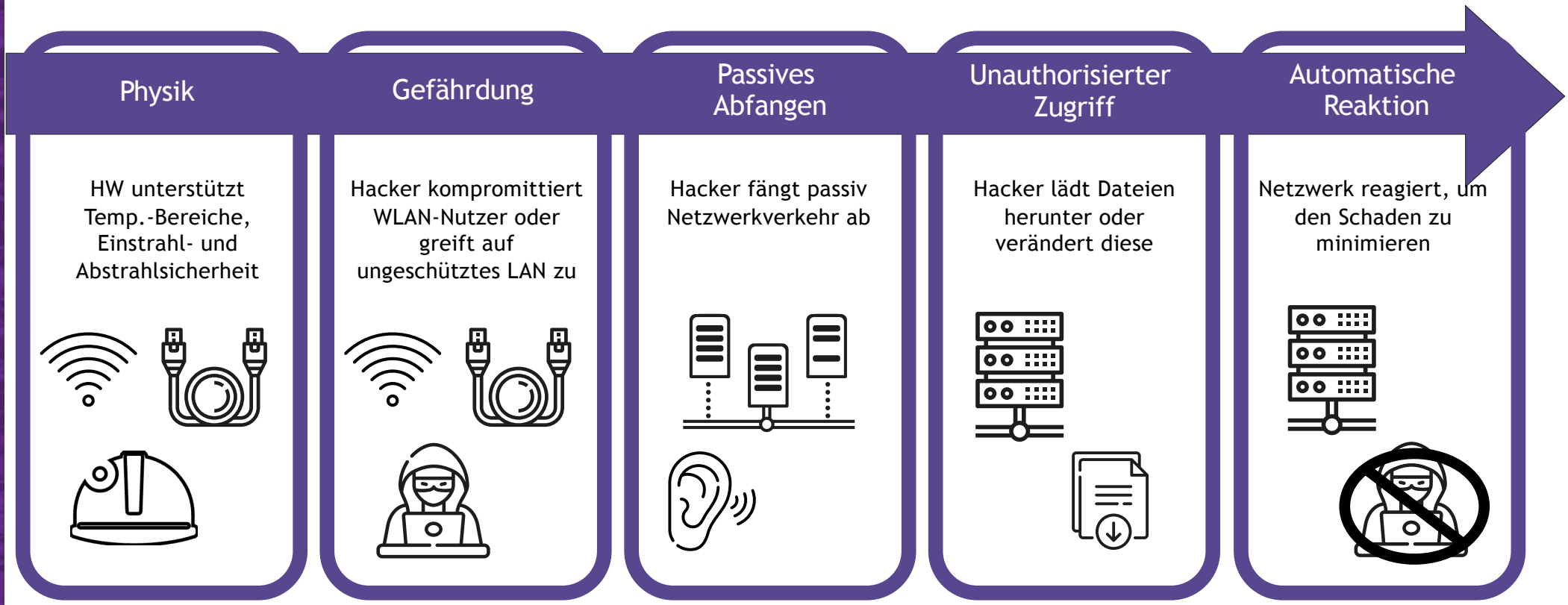
CERTIFIED MILITARY GRADE Drop-Tested MIL-STD 810G-516.6 U.S.A.

Marine

CERTIFIED BY DNV·GL MARITIME

Alcatel·Lucent Enterprise

NETZWERKSICHERHEIT UMFASST VERSCHIEDENE BEREICHE



VERTRAUE NIEMANDEM – DER SICHERSTE ANSATZ

Alcatel·Lucent Enterprise

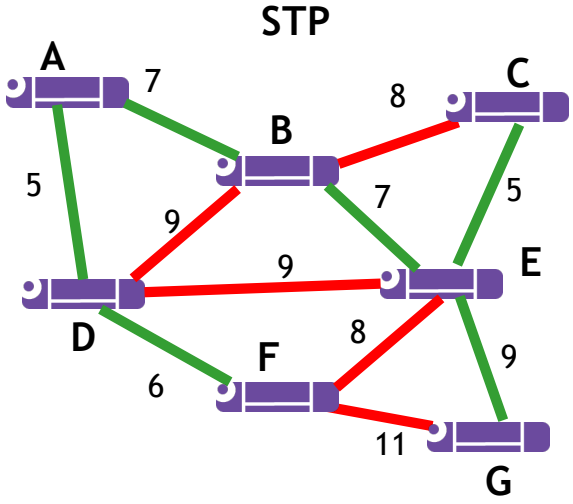
SHORTEST PATH BRIDGING

SERVICEEBENEN FÜR DAS NETZWERK

STP VS SPB-M

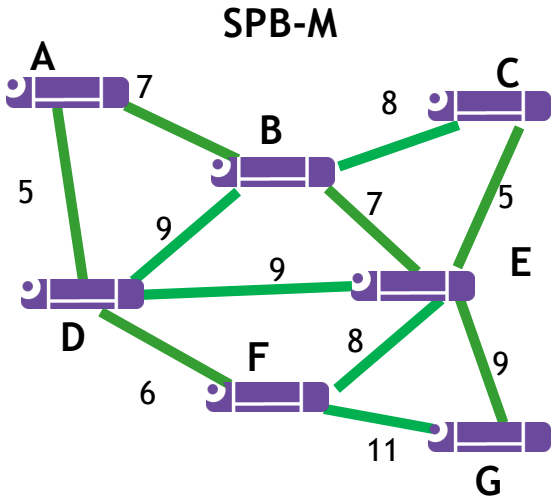
Spanning Tree Protokoll

- Eine Baumstruktur, der Datenverkehr muss durch die “Root Bridge”
- F zu G benötigt fünf Hops, obwohl eine direkte Nachbarschaft besteht
- Viele blockierte Pfade, Bandbreite liegt brach



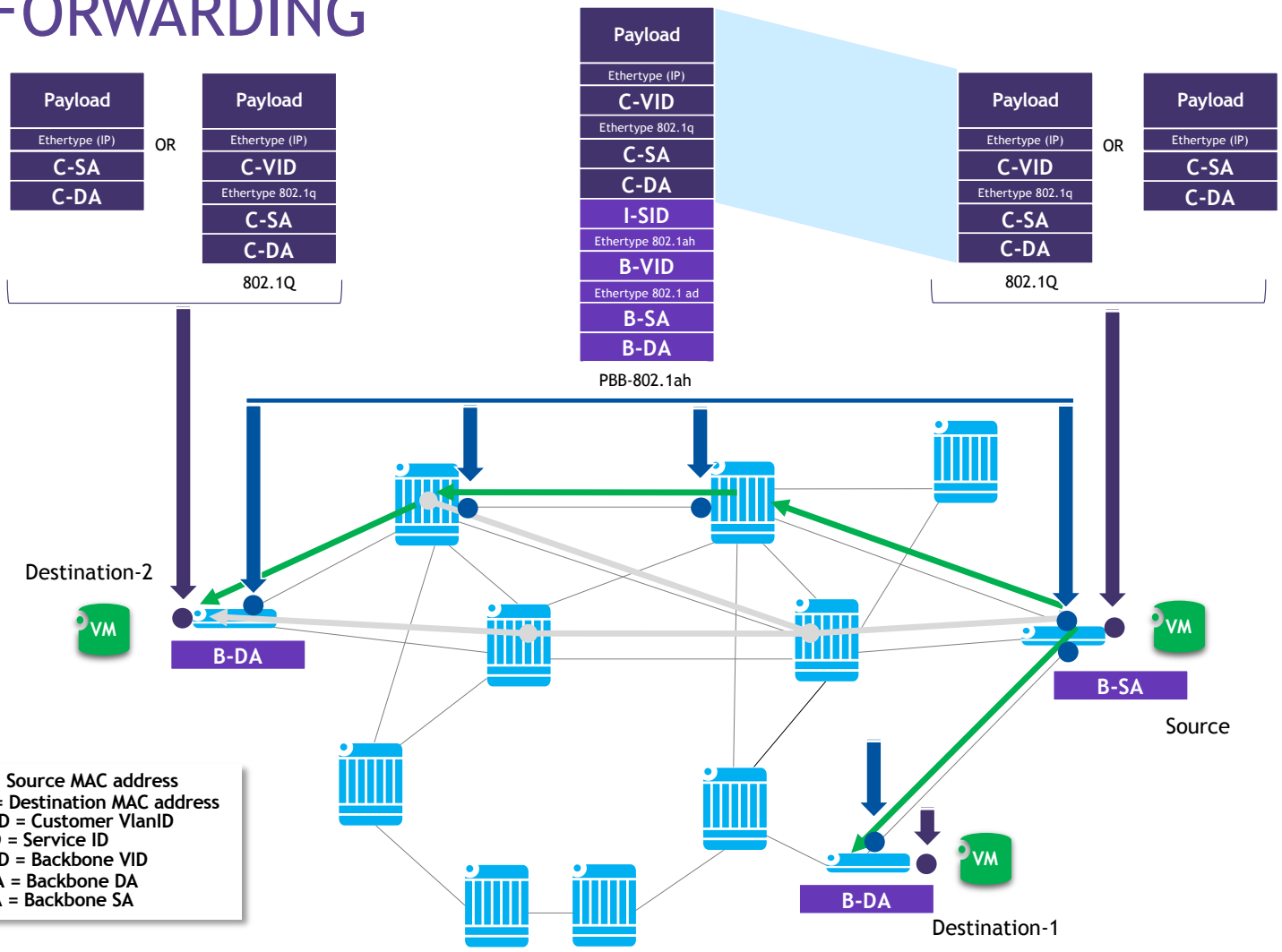
Shortest-Path-Bridging

- Jeder Switch ist seine eigene Root Bridge mit symmetrischen Pfaden
- Datenverkehr nutzt den kürzesten Pfad
- Service-Isolation durch MAC-in-MAC
- Mesh-Topologien
- Keine Loops
- Schnelle Wiederherstellung



Alcatel·Lucent Enterprise

SHORTEST PATH BRIDGING DATA FORWARDING



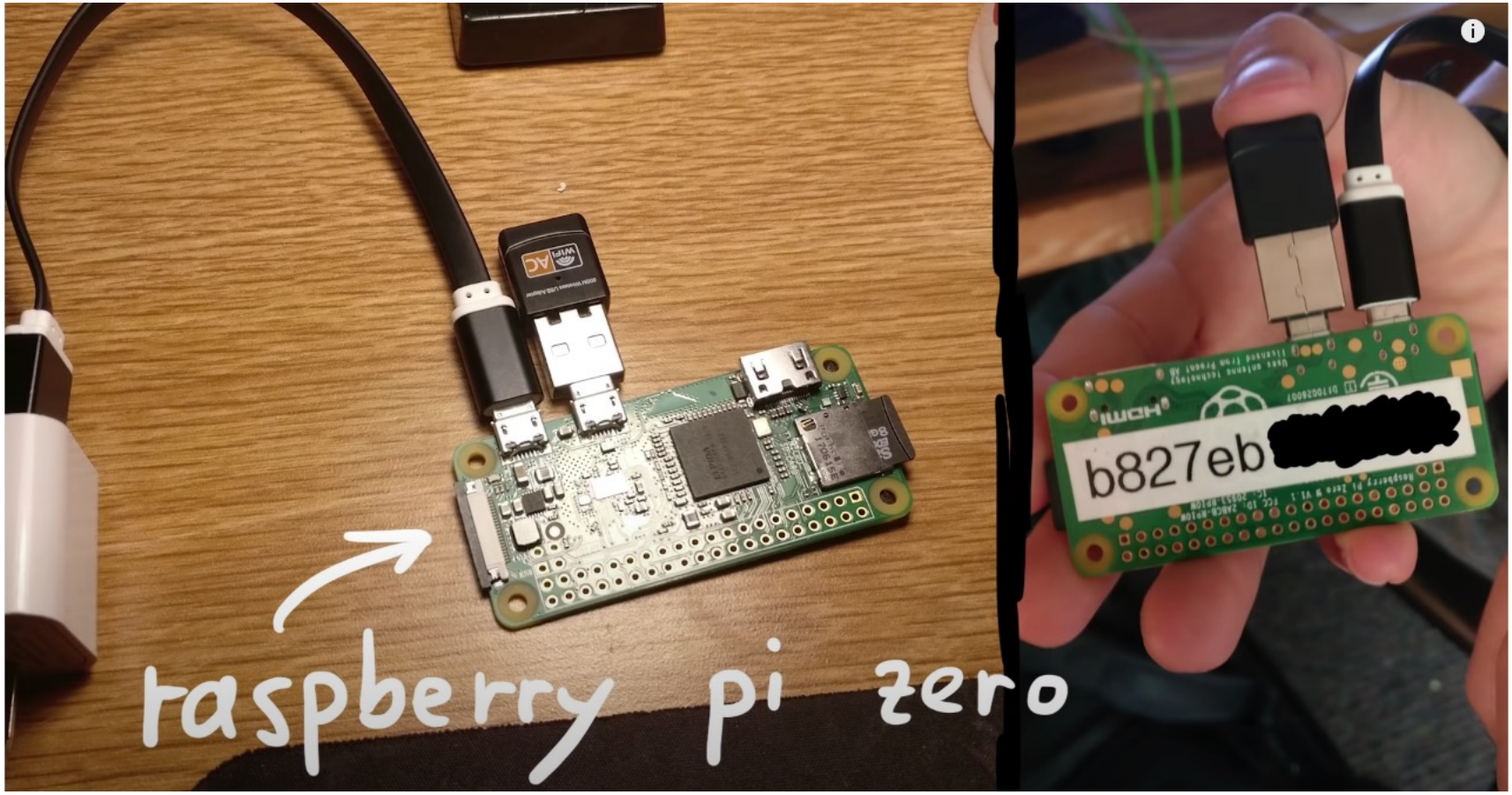
Alcatel·Lucent Enterprise

ZUGANGSKONTROLLE UND IOT

WER? WAS? IOT INVENTAR!

ROLLENBASIERTER NETZWERKZUGANG

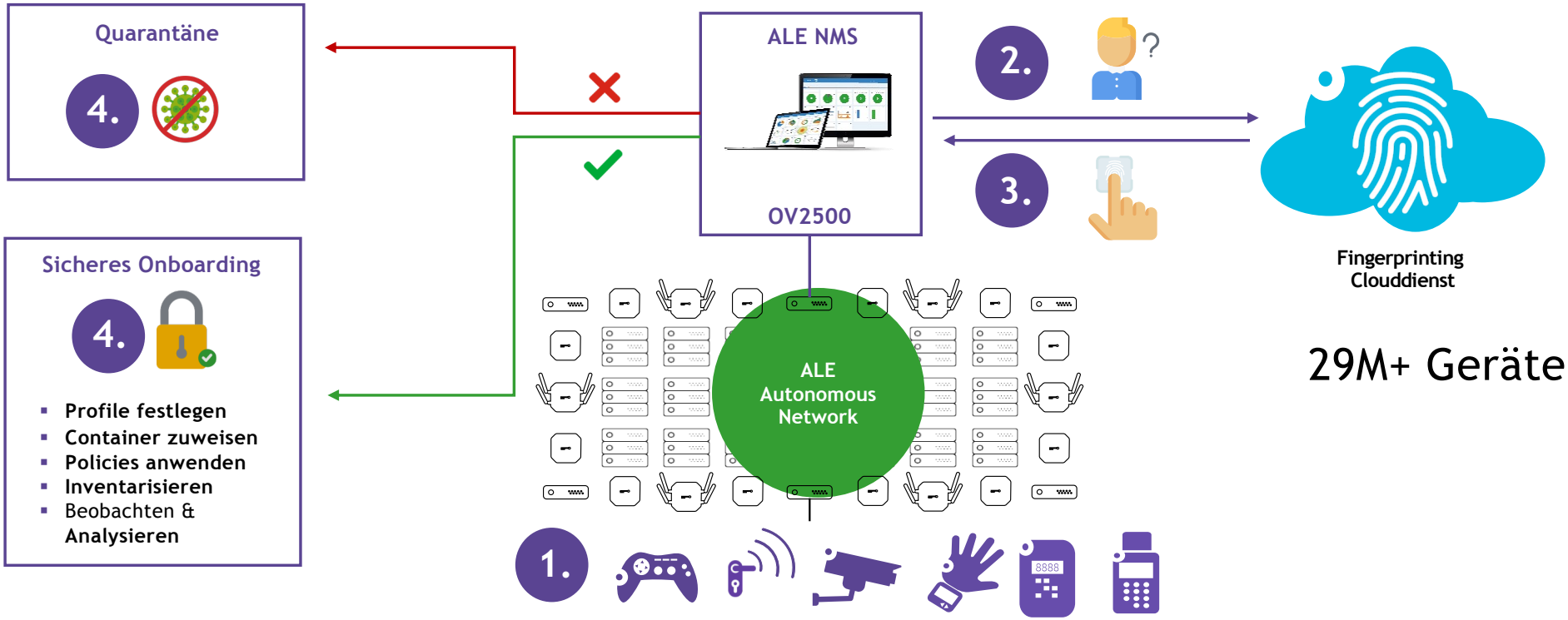
Ihr Netzwerk ist durch NAC geschützt oder?



Alcatel·Lucent Enterprise

AUTOMATISIERUNG - IOT SECURED ONBOARDING

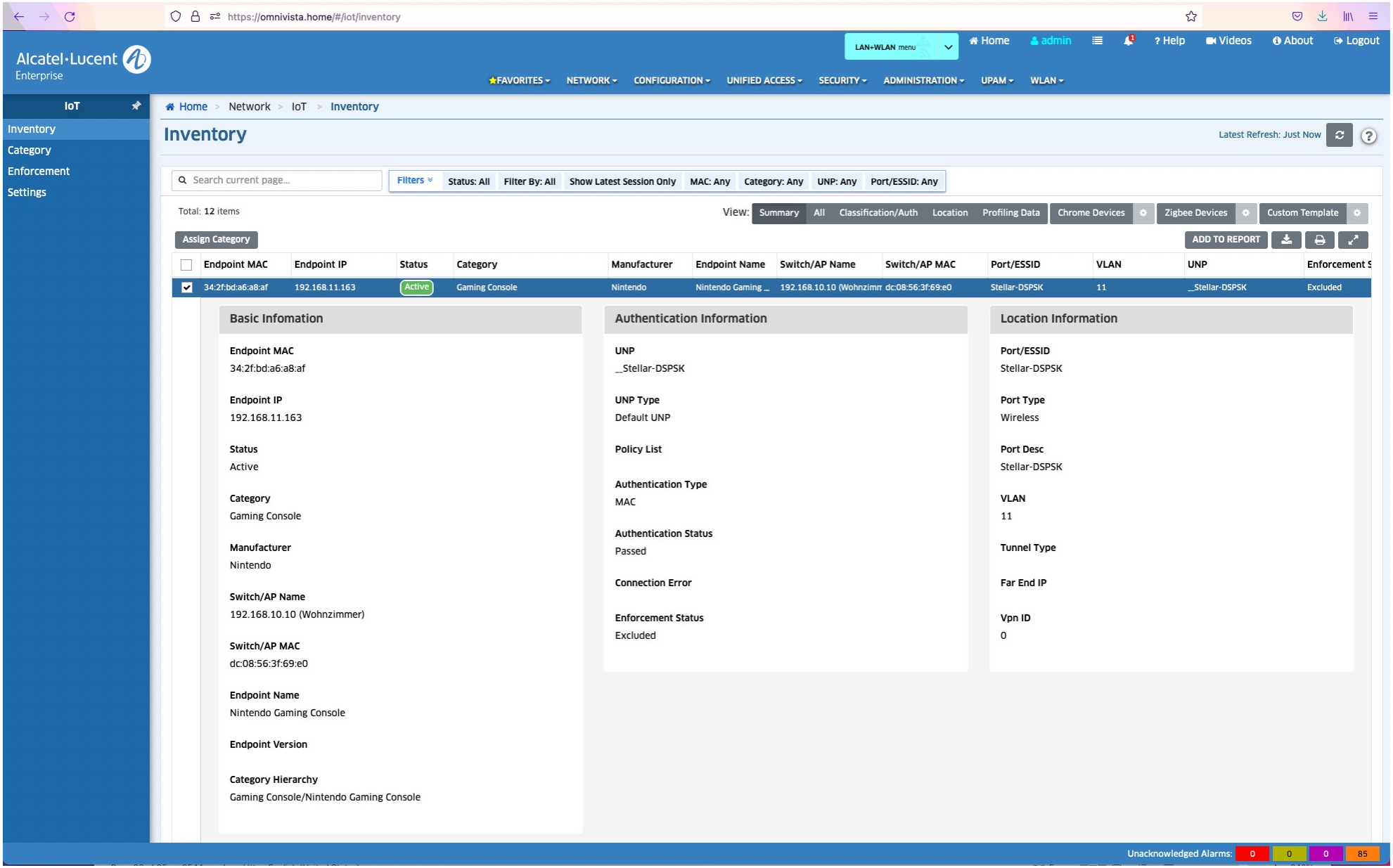
Exemplarische Einbindung von IoT Geräten



29M+ Geräte

Selbst IoT Geräte lassen sich nun sicher einbinden!

Alcatel·Lucent Enterprise

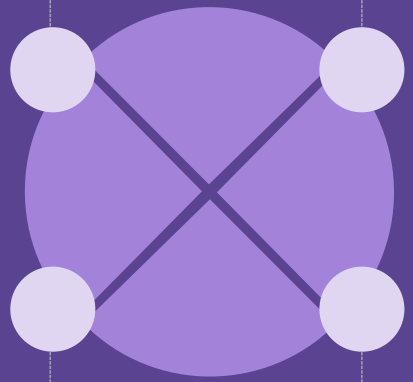

https://omnivista.home/#/iot/inventory
Alcatel·Lucent Enterprise
LAN+WLAN menu
Home
admin
Help
Videos
About
Logout
FAVORITES
NETWORK
CONFIGURATION
UNIFIED ACCESS
SECURITY
ADMINISTRATION
UPAM
WLAN
IoT
Inventory
Category
Enforcement
Settings
Home > Network > IoT > Inventory
Inventory
Latest Refresh: Just Now
Search current page...
Filters
Status: All
Filter By: All
Show Latest Session Only
MAC: Any
Category: Any
UNP: Any
Port/ESSID: Any
Total: 12 items
View:
Summary
All
Classification/Auth
Location
Profiling Data
Chrome Devices
Zigbee Devices
Custom Template
Assign Category
ADD TO REPORT
Endpoint MAC
Endpoint IP
Status
Category
Manufacturer
Endpoint Name
Switch/AP Name
Switch/AP MAC
Port/ESSID
VLAN
UNP
Enforcement S
34:2f:bd:a6:a8:af
192.168.11.163
Active
Gaming Console
Nintendo
Nintendo Gaming ...
192.168.10.10 (Wohnzimm
dc:08:56:3f:69:e0
Stellar-DSPSK
11
_Stellar-DSPSK
Excluded
Basic Infomation
Endpoint MAC
34:2f:bd:a6:a8:af
Endpoint IP
192.168.11.163
Status
Active
Category
Gaming Console
Manufacturer
Nintendo
Switch/AP Name
192.168.10.10 (Wohnzimmer)
Switch/AP MAC
dc:08:56:3f:69:e0
Endpoint Name
Nintendo Gaming Console
Endpoint Version
Category Hierarchy
Gaming Console/Nintendo Gaming Console
Authentication Information
UNP
_Stellar-DSPSK
UNP Type
Default UNP
Policy List
Authentication Type
MAC
Authentication Status
Passed
Connection Error
Enforcement Status
Excluded
Location Information
Port/ESSID
Stellar-DSPSK
Port Type
Wireless
Port Desc
Stellar-DSPSK
VLAN
11
Tunnel Type
Far End IP
Vpn ID
0
Unacknowledged Alarms:
0
0
0
85

UNIFIED POLICY AUTHENTICATION MANAGER (UPAM)

FERTIGE LÖSUNG FÜR DEN SICHEREN NETZWERKZUGANG

Authentifizierung

- Active Directory/LDAP mit Role Mapping
- Eingebauter Radius (mit Attributen)
- Proxy zu externen Radius Servern
- Device-Specific PSK
- Authenticated Switch Access
- Personal Group PSK



Gäste

- Mehrere Gaststrategien möglich
- Flexibel: Selbstregistrierung oder Freigabe durch besuchten Mitarbeiter. Notification via SMS, Web, Email
- Anmeldung: Benutzername/Passwort, Zugangscode, AGBs, Social Login
- Festlegen des Servicelevel (z.B. Basic/Premium/VIP)
- Wahlweise Abfrage von kundenspezifischen Angaben

Rainbow™

Captive Portal

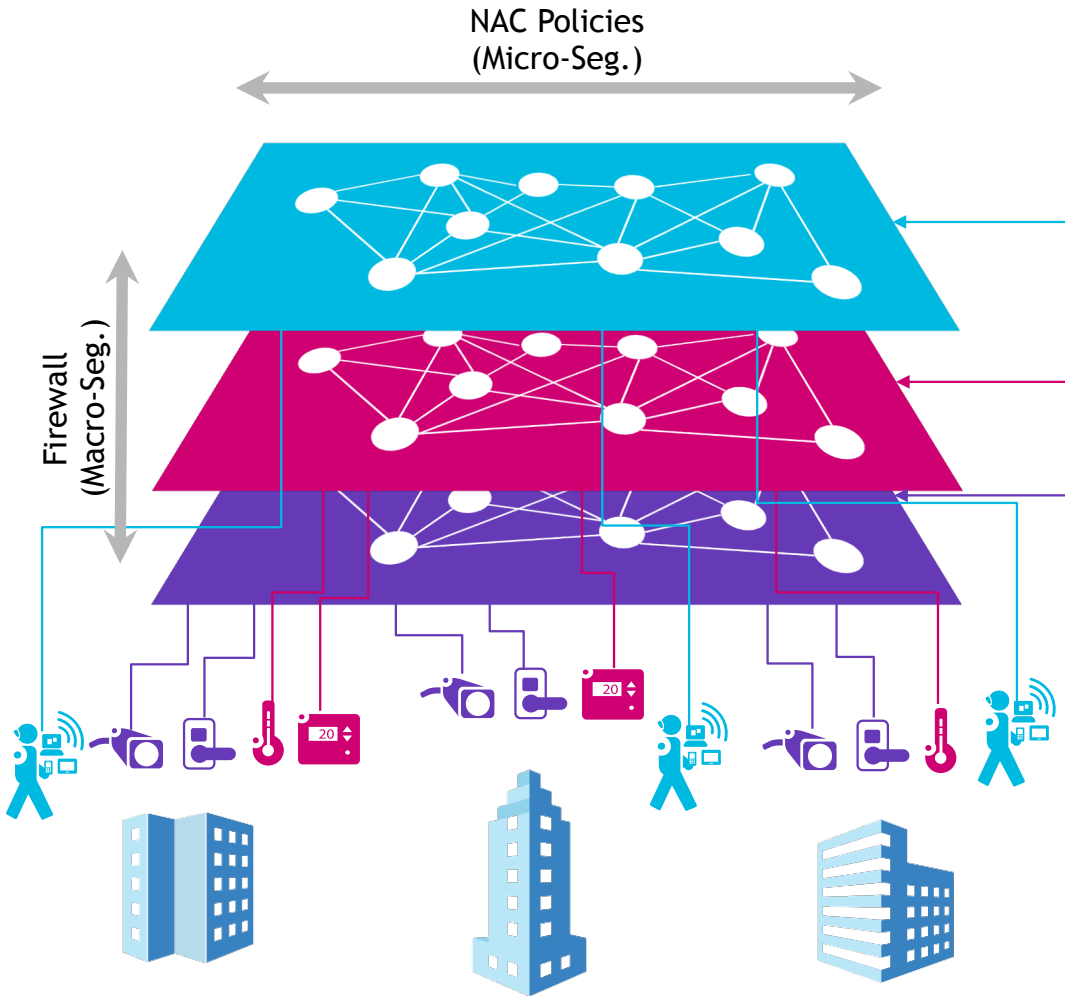
- Editierbare Seiten
- Weiterleitungs URL

BYOD

- Mehrere BYOD Strategien möglich
- Session- & Gerätekontrolle

Flexible und vielseitige NAC-Lösung mit integriert!

MACRO- vs MICRO-SEGMENTIERUNG



Nutzer

- ✓ Authentifizieren
- ✓ Klassifizieren
- ✓ Bereitstellen

✓Sicherheit ✓Qualität | ✓Sicherheit ✓Qualität

Heizung, Lüftung, Klimatechnik

- ✓ Authentifizieren
- ✓ Klassifizieren
- ✓ Bereitstellen

✓Sicherheit ✓Qualität | ✓Sicherheit ✓Qualität

Gebäude-/Campussicherheit

- ✓ Authentifizieren
- ✓ Klassifizieren
- ✓ Bereitstellen

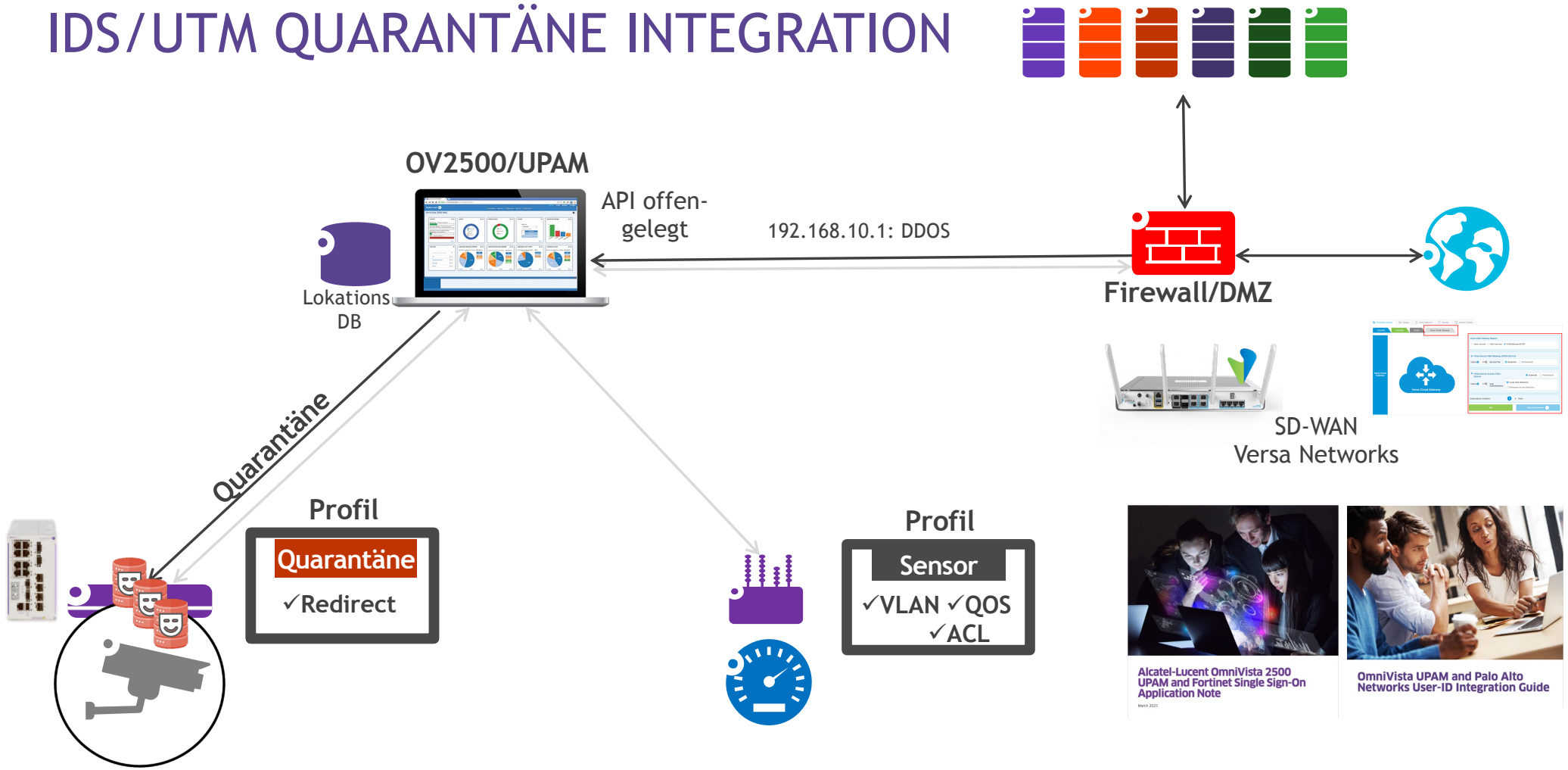
✓Sicherheit ✓Qualität | ✓Sicherheit ✓Qualität

Alcatel·Lucent Enterprise

ANOMALIEN IM NETZWERK

WIE ERKENNEN? WAS TUN? WER MELDET/ERKENNT?

IDS/UTM QUARANTÄNE INTEGRATION



Alcatel·Lucent
Enterprise

OMNIVISTA NETWORK ADVISOR

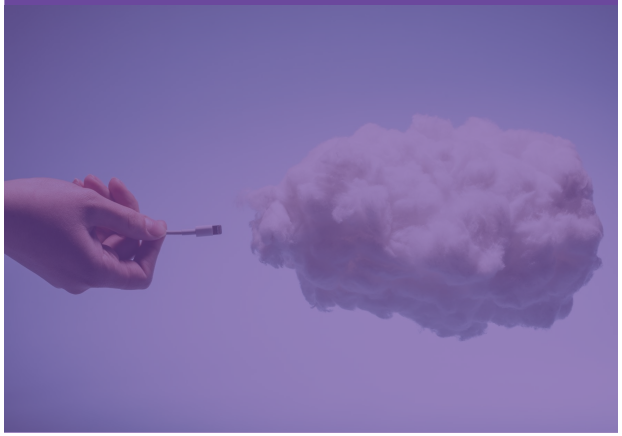
DER NETZWERKBERATER IN DER WESTENTASCHE

Alcatel·Lucent
Enterprise

DIGITAL AGE STRATEGY

CLOUD

Digital Age Cloud Strategy



NETZWERK

Digital Age Network Strategy

KOMMUNIKATION

Digital Age Communication Strategy

Alcatel·Lucent
Enterprise

DIGITAL AGE STRATEGY

CLOUD

Digital Age Cloud Strategy

NETZWERK

Digital Age Network Strategy

KOMMUNIKATION

Digital Age Communication Strategy

Alcatel·Lucent
Enterprise

OMNIVISTA NETWORK ADVISOR

AI(OPS) / ML

Alcatel·Lucent
Enterprise

ZEIT SPAREN

Alcatel·Lucent
Enterprise

ALE TECHNICAL KNOWLEDGE BASE

IDENTIFIZIEREN


LÖSEN

OPTIMIEREN


VIELSEITIG

OMNIVISTA NETWORK ADVISOR

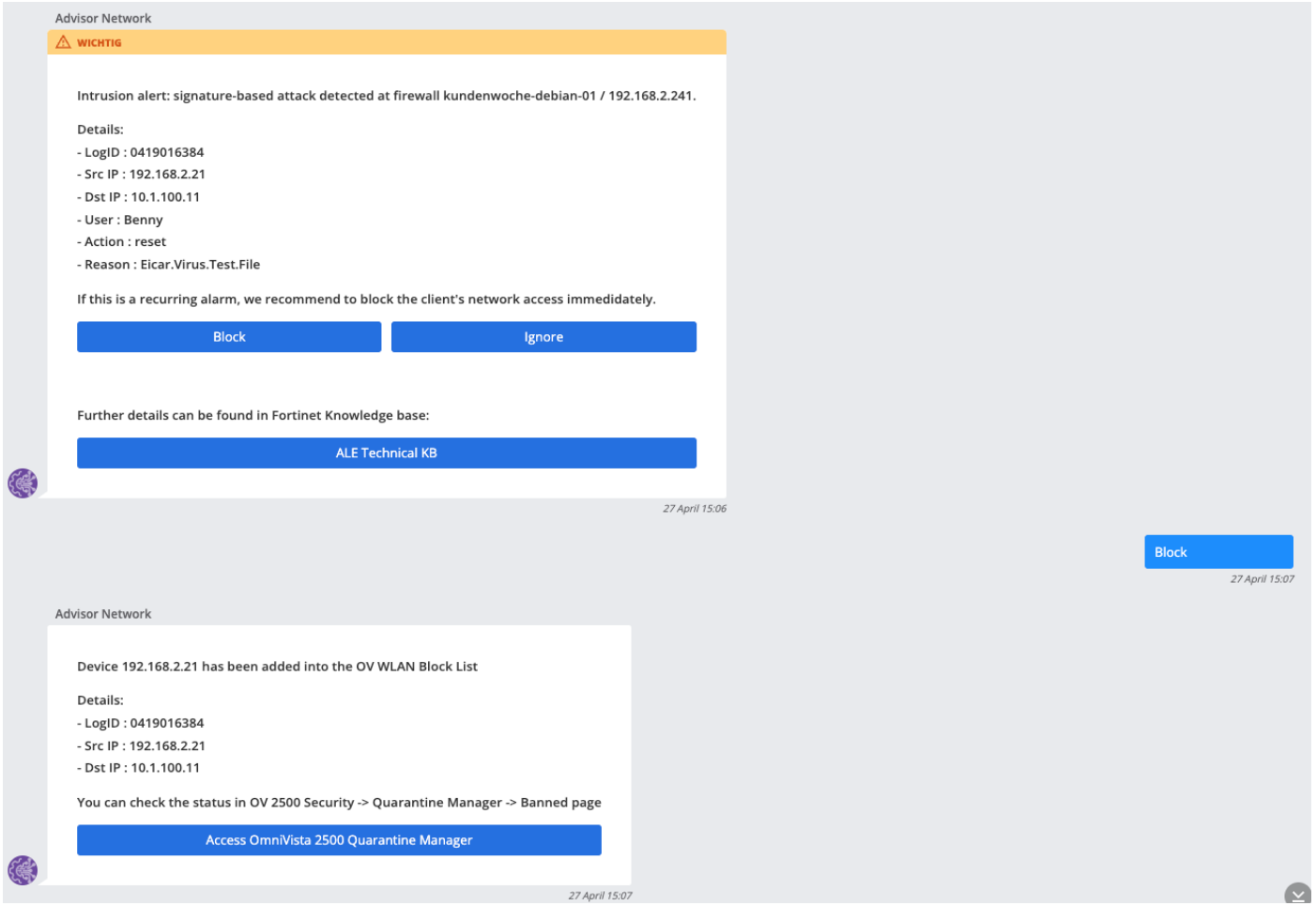
DER LANGE ARM DES GESETZES

Alcatel·Lucent
Enterprise

FORTINET MELDUNG

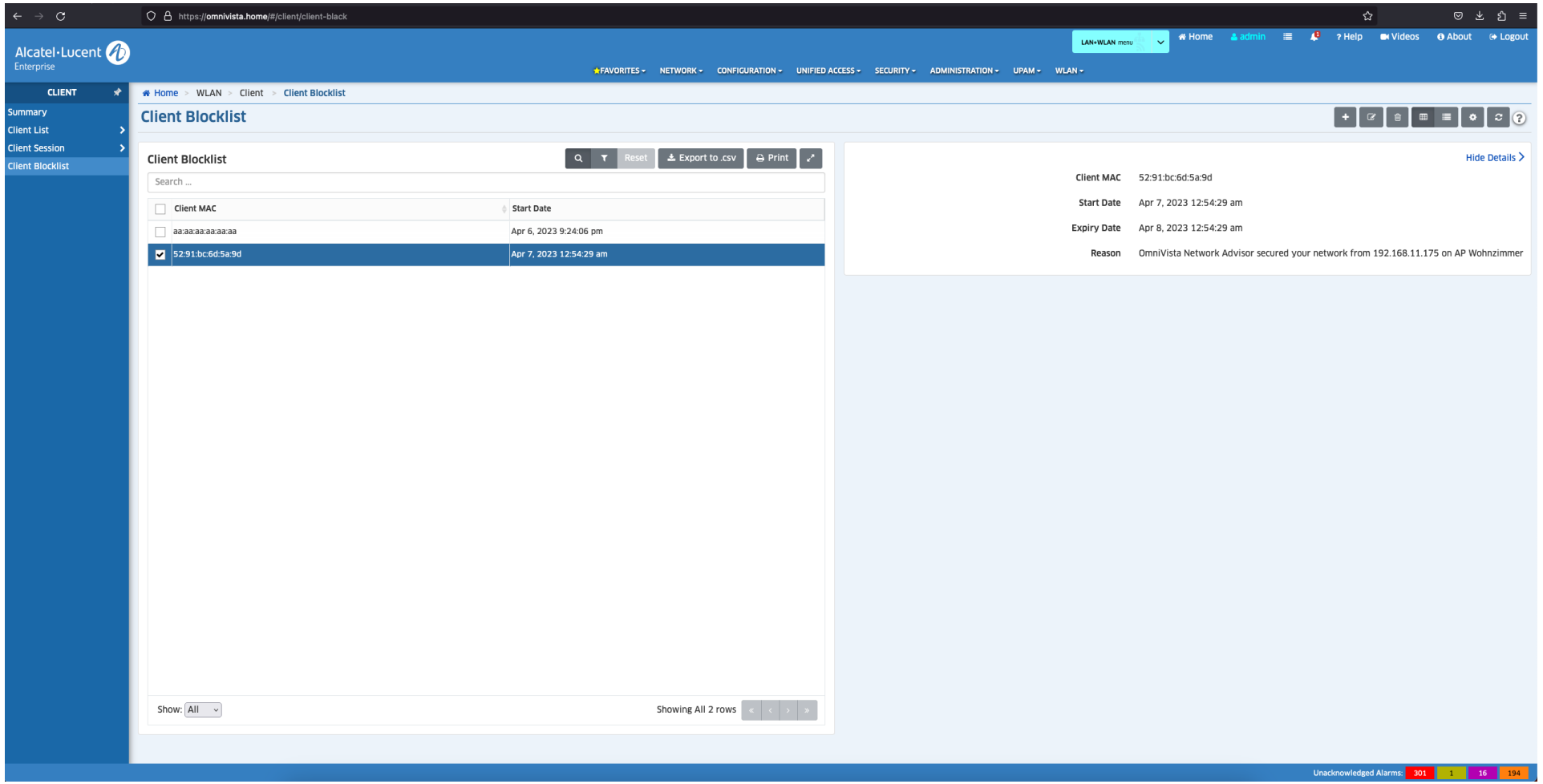
- logger -d -n 192.168.2.243 -P 10514 **logid=\"0419016384\"** type="utm" subtype="ips" **attack=\"Eicar.Virus.Test.File\"** severity="info" **srcip=192.168.2.21** srccountry="Reserved" dstip=10.1.100.11 ref=\"http://www.fortinet.com/ids/VID29844\" **user=\"Benny\"** dstintfrole="undefined" sessionid=901 **action=\"reset\"** proto=6 service="HTTP" policyid=1 srcport=80 dstport=44362 hostname="172.16.200.55" url="/virus/eicar.com" direction="incoming" attackid=29844 profile="test-ips" incidentserialno=877326946 msg="file_transfer: Eicar.Virus.Test.File,"

OMNIVISTA NETWORK ADVISOR



Alcatel·Lucent Enterprise

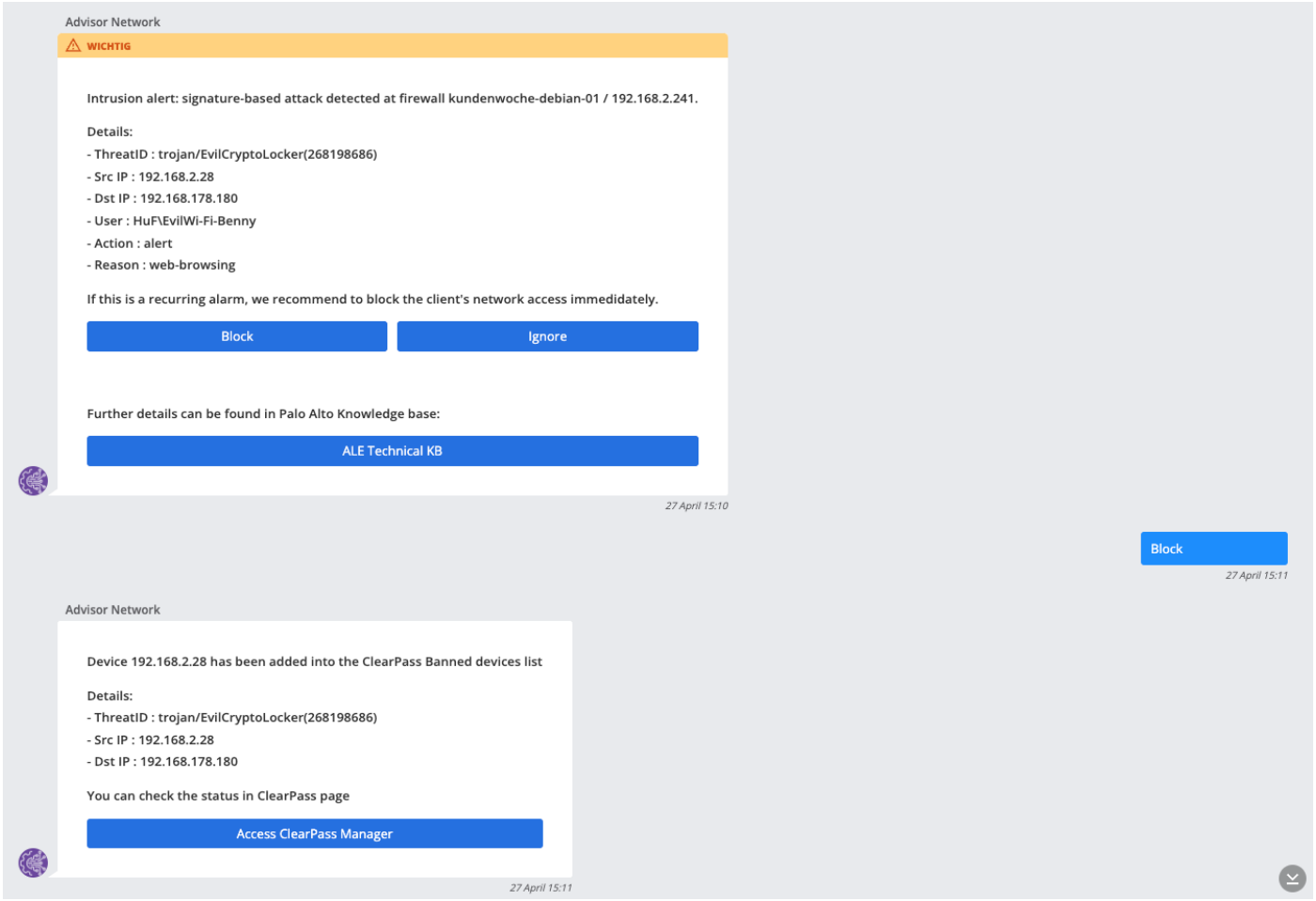
OMNIVISTA NETWORK ADVISOR



PALO ALTO MELDUNG

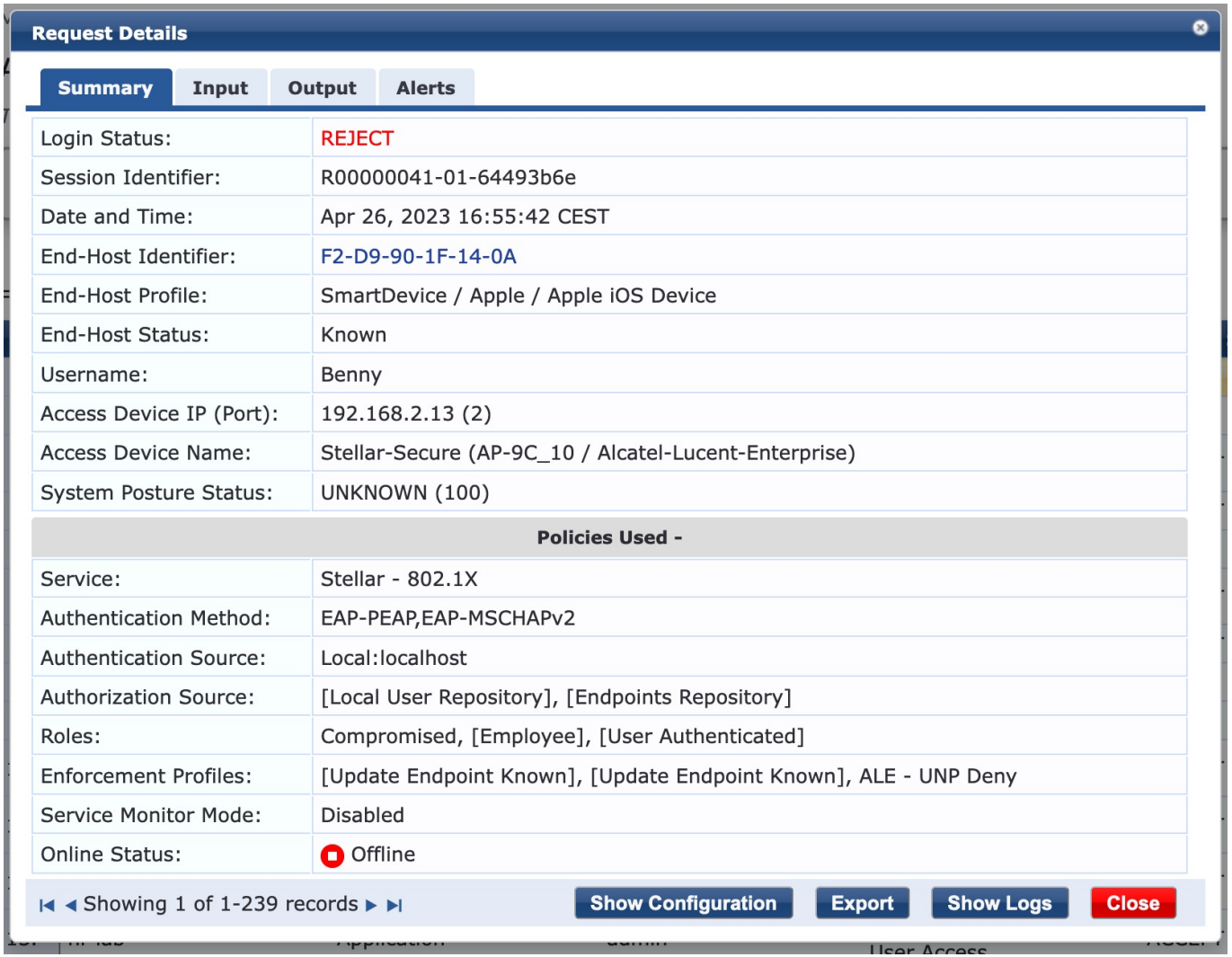
- logger -d -n 192.168.2.243 -P 10514 '<180>May 6 16:43:53 paloalto.paseries.test LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|8.1.6|trojan/PDF.gen.eiez(268198686)|ReceiveTime=2019/05/06 16:43:53|SerialNumber=001801010877|cat=THREAT|Subtype=virus|devTime=May 06 2019 11:13:53 GMT|**src=192.168.2.28**|dst=192.168.178.180|srcPostNAT=192.168.68.141|dstPostNAT=192.168.178.180|RuleName=Test-1|**usrName=HuF\\EvilWi-Fi-Benny**|SourceUser=qradar\\user1|DestinationUser=|Application=web-browsing|VirtualSystem=vsys1|SourceZone=INSIDE-ZN|DestinationZone=OUTSIDE-ZN|IngressInterface=ethernet1/1|EgressInterface=ethernet1/3|LogForwardingProfile=testForwarder|SessionID=3012|RepeatCount=1|srcPort=63508|dstPort=80|srcPostNATPort=31539|dstPostNATPort=80|Flags=0x406000|proto=tcp|action=alert|Miscellaneous=\"qradar.example.test/du/uploads/08052018_UG_FAQ.pdf\"|**ThreatID=trojan/EvilCryptoLocker(268198686)**|URLCategory=educational-institutions|sev=3|Severity=medium|Direction=server-to-client|sequence=486021038|ActionFlags=0xa000000000000000|SourceLocation=10.0.0.0-10.255.255.255|DestinationLocation=testPlace|ContentType=|PCAP_ID=0|FileDigest=|Cloud=|URLIndex=5|RequestMethod=|Subject=|DeviceGroupHierarchyL1=12|DeviceGroupHierarchyL2=0|DeviceGroupHierarchyL3=0|DeviceGroupHierarchyL4=0|vSrcName=|DeviceName=testName|SrcUUID=|DstUUID=|TunnelID=0|MonitorTag=|ParentSessionID=0|ParentStartTime=|TunnelType=N/A|ThreatCategory=pdf|ContentVer=Antivirus-2969-3479'

OMNIVISTA NETWORK ADVISOR



Alcatel·Lucent Enterprise

CLEARPASS



Alcatel·Lucent Enterprise

CONTACT US

WEBSITE

www.al-enterprise.com

Follow us on:

Alcatel·Lucent Enterprise

Alcatel·Lucent
Enterprise