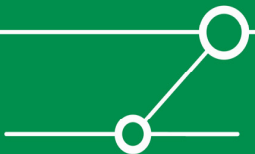


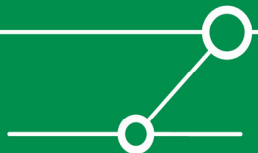
Werkzeuge zur technischen Umsetzung von Security Policy Compliance

Dror-John Röcher
droecher@ernw.de
www.ernw.de



Was ist Security Policy Compliance?

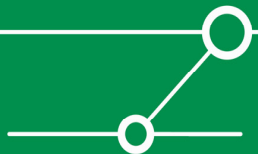
- Betrachtet wird in diesem Kontext gerade nicht die „Compliance“ in Bezug auf [externe] Gesetze/Vorschriften & Standards. Das wurde in den vorhergehenden Vorträgen ausführlich beleuchtet.
- „Security Policy Compliance“ bezieht sich auf den Grad der **Einhaltung interner Richtlinien** und insbesondere auf den Grad der **Einhaltung der Security Policy**.
- Allerdings ist die Ausgestaltung der internen Richtlinien & Security Policies stark geprägt von Gesetzen/Vorschriften & Standards. Hier schließt sich der Kreis wieder.

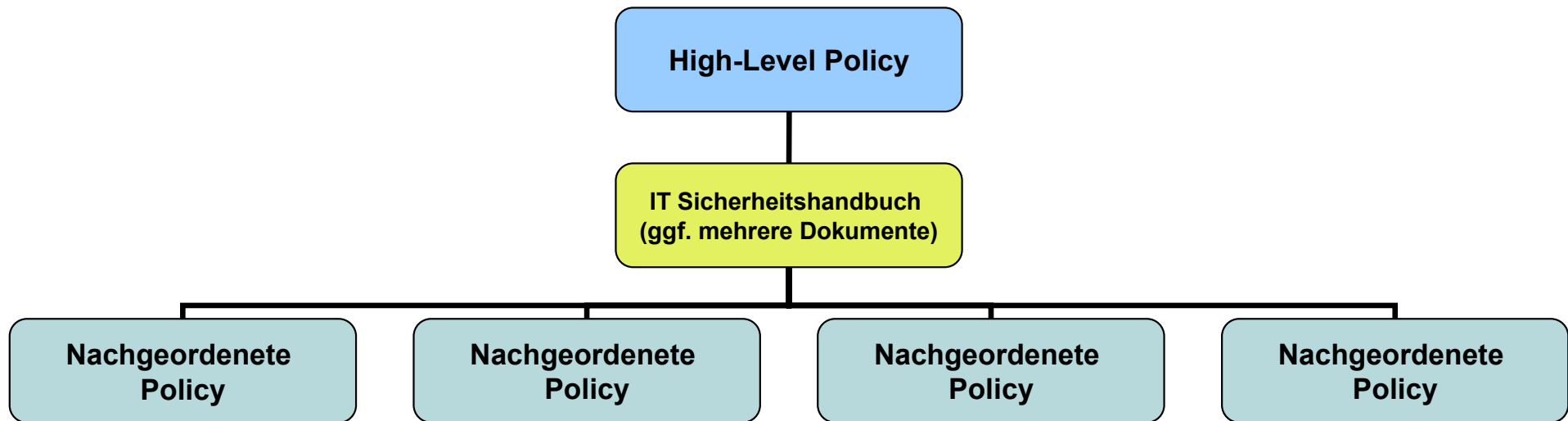


Die Corporate IT-Security Policy

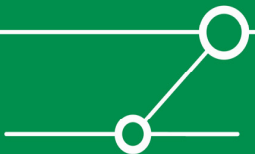
■ ISO/IEC 17799:2005, Section 5.1:

- The information security policy document should state management commitment and set out the organization's approach to managing information security.
- This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.



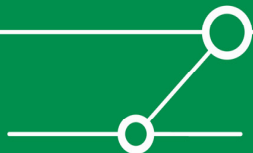


- Die Dokumentenstruktur ermöglicht
 - Änderungen in Teilbereichen, ohne andere Bereiche zu beeinträchtigen
 - Aufteilung von Verantwortlichkeiten (Document-Owner)
 - Review von Teilbereichen
 - Vereinfachte (elektronische & gedruckte) Publikation und Kommunikation



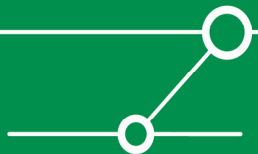
Dieses Dokument ist i.a. **nicht** aufwendig, aber **höchst** wichtig!

- Die Ziele einer Organisation zur Informationssicherheit und ihre Bedeutung für die Organisation
- Die wichtigsten Prinzipien, Standards und Verpflichtungen zur Informationssicherheit
- Die Festlegung von Verantwortlichkeiten (in generischer Form) für wichtige Aspekte der Informationssicherheit
- Verweise auf Dokumente mit detaillierten Verfahrensbeschreibungen, Regelungen, Organisationsstrukturen etc.



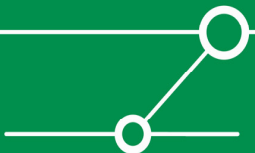
Fragen, die (kurz!) beantwortet werden sollten:

- Wodurch wird der Geschäftszweck erreicht?
- Welche Rolle spielt darin die IT?
- Weshalb ist dann IT-Security wichtig?
- Welche elementaren Ziele sind bedroht?
- Welche (gesetzlichen) Rahmenbedingungen sind zu beachten?
- Für wen gilt die Policy & wer ist für IT-Sicherheit zuständig?



Kernpunkte einer Endpunkt-Security Policy

- Die Endpunkt-Security Policies lassen sich häufig auf 3 (einfache?) Punkte unterbrechen:
 1. **Patchlevel:** Systeme müssen zeitnah gepatcht werden. Die Freigabe der Patches erfolgt durch einen zentralen Dienst.
 2. **Malicious Code:** Systeme müssen mit einer aktuellen AntiViren/AntiSpyware/AntiTrojaner Lösung versehen sein. Die Software wird zentral zur Verfügung gestellt, Updates der ScanEngine und der Signaturen erfolgen über einen zentralen Dienst.
 3. **Unwanted Programs:** Alle Programme, die nicht auf der „Corporate Whitelist“ stehen, sind automatisch „unerwünscht“ und dürfen nicht auf den Systemen installiert sein. Software-Installation erfolgt ausschließlich durch die zentrale IT-Abteilung.

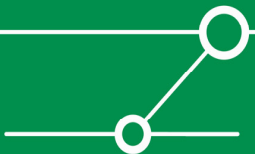


Bedrohungen durch Endpunkte

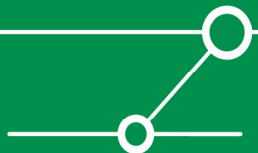
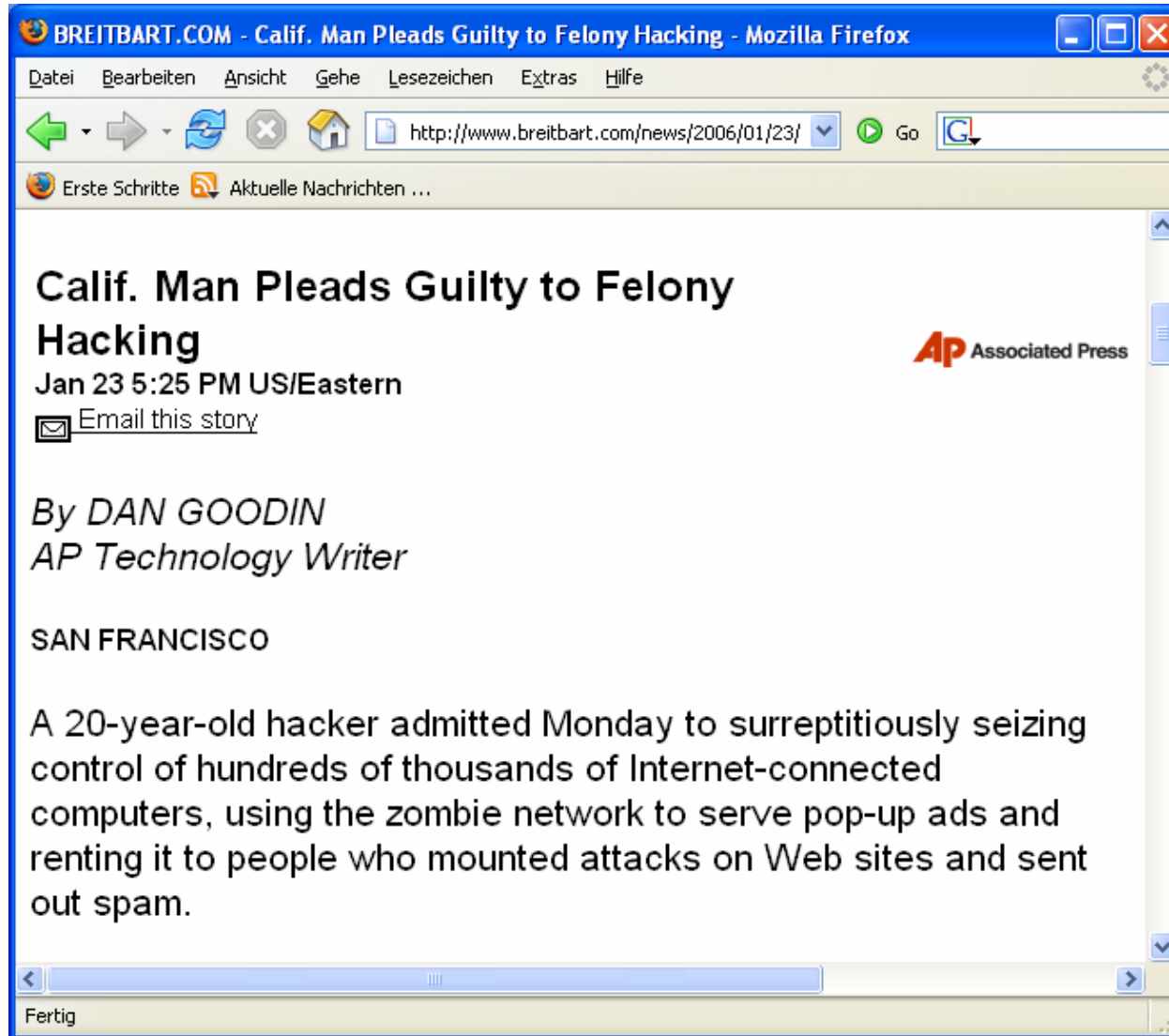
- Verfügbarkeit von Systemen/Netzen/Daten
 - Z.B. Verfügbarkeit des Netzwerkes bei SQL-Slammer Ausbruch.
 - Z.B. Verfügbarkeit von Daten, die durch einen Virus gelöscht wurden (aktuell: „blackworm“, aka „nyxem“, aka „kama sutra“)

- Vertraulichkeit von Daten
 - Spyware sammelt Benutzerverhalten, Passwörter, Zugangskennungen ein.
 - Speziell angepasster Malicious Code sammelt gezielt vertrauliche Dokumente eines dedizierten Opfers (Stichwort: Wirtschaftsspionage).

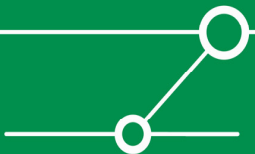
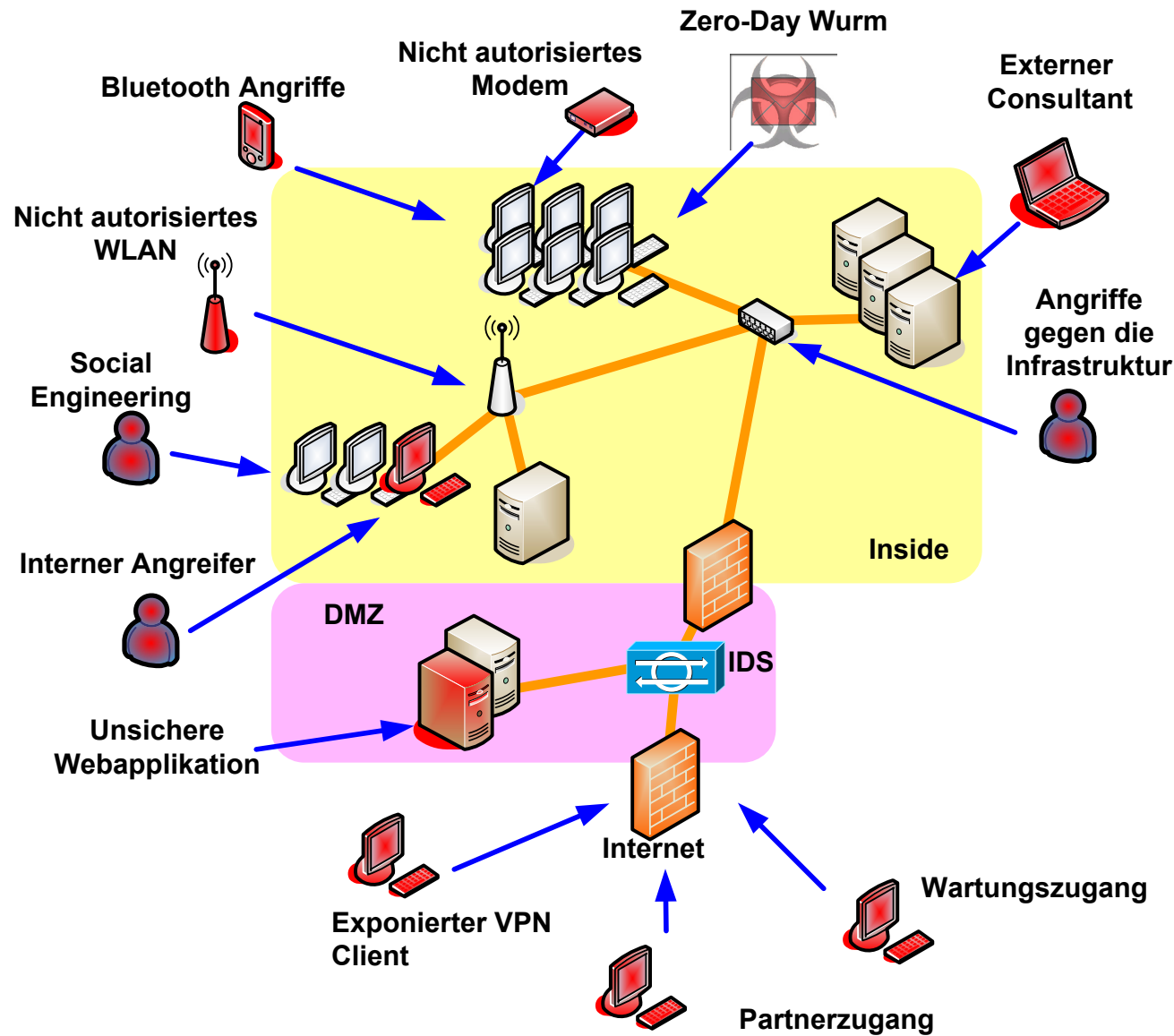
- Missbrauch von Ressourcen
 - Gehackter Endpunkt als Relay für weitere Angriffe.
 - Gehackter Endpunkt als Knoten eines Botnet (Spam-Schleuder, DDoS Plattform, Stealth-Hosting)



Beispiel „BotNet“



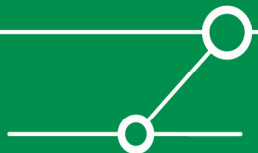
Einige Bedrohungen im Überblick



Welche Systeme sind Compliant?

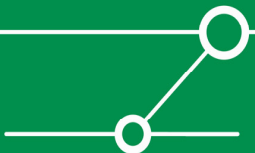
- Aus den vorgenannten Kernpunkten lassen sich folgende quantitativen Metriken für die Compliance eines einzigen Systems ableiten:
 - Wieviele Patches fehlen auf dem System?
 - Wieviele AV-Signatur-Updates fehlen auf dem System?
 - Wieviele ScanEngine-Updates fehlen auf dem System?
 - Wieviele „unerwünschte“ Programme auf dem System sind installiert?

- Diese quantitativen Metriken können sowohl im ITIL Kontext als z.B. auch als „key performance indicator“ im ISO 17799 benutzt werden um den „Grad der Compliance“ zu messen.



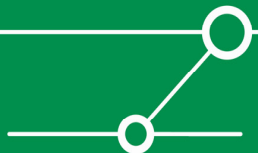
„non-compliant“ Systeme...

- Für Patchmanagement, AV & Softwareinstallation existieren ausgereifte Produkte mit zentralisierten Managementschnittstellen. Trotzdem existieren in Netzwerken Systeme, auf denen aktuelle Patches bzw. AV-Signaturen fehlen oder auf denen unerwünschte Software (z.B. Skype) installiert ist.
- Kategorien von „non-compliant“ Systemen:
 - Außendienstmitarbeiter mit sporadischer Verbindung ins Unternehmensnetz.
 - Interne Systeme, bei denen Patch & AV versagt haben, oder vom User abgestellt wurden, bzw. auf denen von Usern Software installiert wurde.
 - Interne Systeme, die nicht gepatcht werden können, bzw. auf denen keine AV installiert werden kann. (Telefonanlagen, Steuerungsrechner in der Produktion, Druckserver)
 - Externe Mitarbeiter (Consultants, etc)
 - Systeme an Standorten mit einer anderen/ohne Policy bzw. mit anderen/ohne Patch/AV-Management.
 - von Mitarbeitern mitgebrachte eigene/Heim- PCs, die im Unternehmen angeschlossen werden

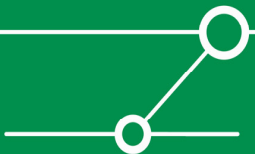


... und wie mit ihnen umgegangen werden kann.

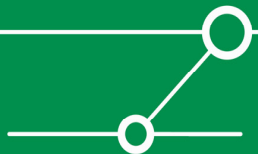
Kategorie	Maßnahme
Interne Systeme & Außendienst	Zugang zu einem Remediation-Portal
Externe Consultants & mitgebrachte Heim-PCs	Zugang zum Gast-LAN mit eingeschränkten Zugriffsrechten
Nicht-patchbare Systeme	Eingeschränkter Netzzugang oder voller Netzzugang
Systeme an anderen Standorten/mit anderer Policy	Eingeschränkter Netzzugang oder voller Netzzugang



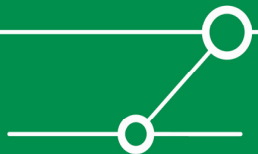
Die Technik....



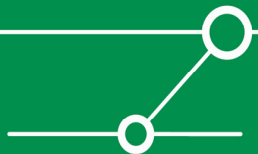
1. Der Zugang zum Netzwerk wird reglementiert anhand des Zustands eines Endpunktes (Policy basierter Zugang):
 - Zugang kann z.B. bedeuten: Guest-VLAN, ACLs auf Routern/Switches, URL-Redirection, Quarantäne
 - Zustand kann z.B. ermittelt werden anhand von: Authentifizierung, installierter Software (AV, Firewall), Patchlevel, installiertem Betriebssystem



2. Das Netzwerk reagiert auf Zustandsänderungen des Endpunktes:
 - Bei Infektion wird das System in Quarantäne genommen.
 - Angriffe auf einen Endpunkt können zu Reaktionen auf anderen Endpunkten führen.

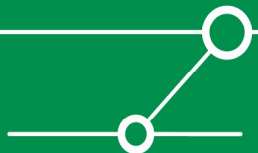


3. Ein Agent überwacht auf Betriebssystem-Kernel-Level alle Aktivitäten:
 - Potentiell schädliche Aktionen werden verhindert, wodurch unbekannte Angriffe oder Viren keine Auswirkungen haben (Schutz vor Zero-Day Angriffen).



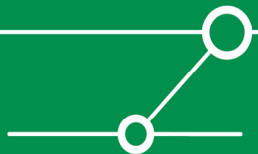
Anforderungen an Lösungen

- Zentrales Management
- Definition von Whitelists (e.g. der „wichtigste“ Server sollte nicht durch einen dummen Zufall vom Netz ausgesperrt wird)
- Integration in bestehende (Netzwerk)-Infrastruktur.
- Integration in bestehende Prozesse.
- Untersuchung von Systemen mit und ohne Agenten.
- Betriebssystemsupport (nur MS, oder auch Unix, Linux, MacOS?)
- Auto-Remediation um den administrativen Aufwand zu minimieren.
- Zusammenarbeit mit Produkten unterschiedlicher Hersteller.
- Unterstützung offener Standards / Offenlegung der Schnittstellen.
- Unterstützung der führenden Frameworks (cisco NAC, TCP-TNC, MS NAP)
- Quarantäne & Gast-Netze.
- Temporäre Ausnahmen.
- Skalierbarkeit im Enterprise-Maßstab.

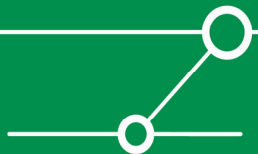
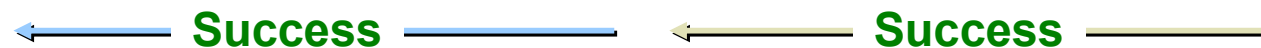
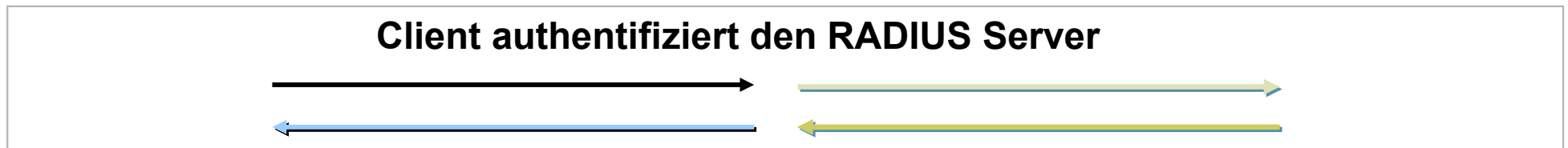
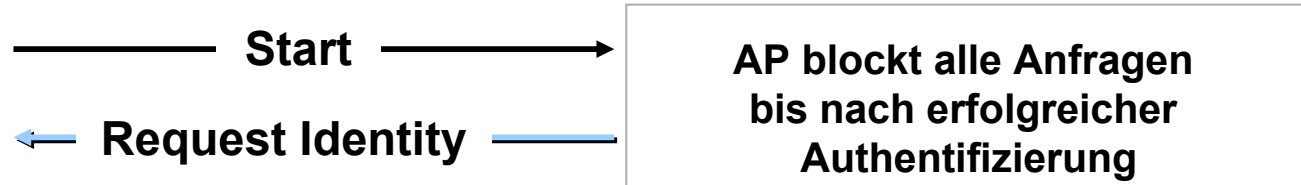
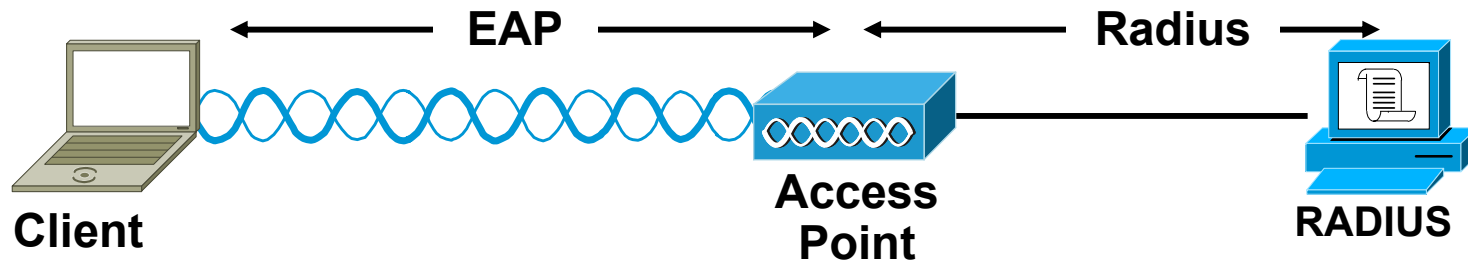


Beispiel

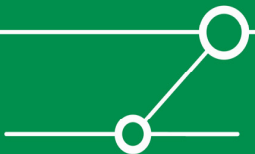
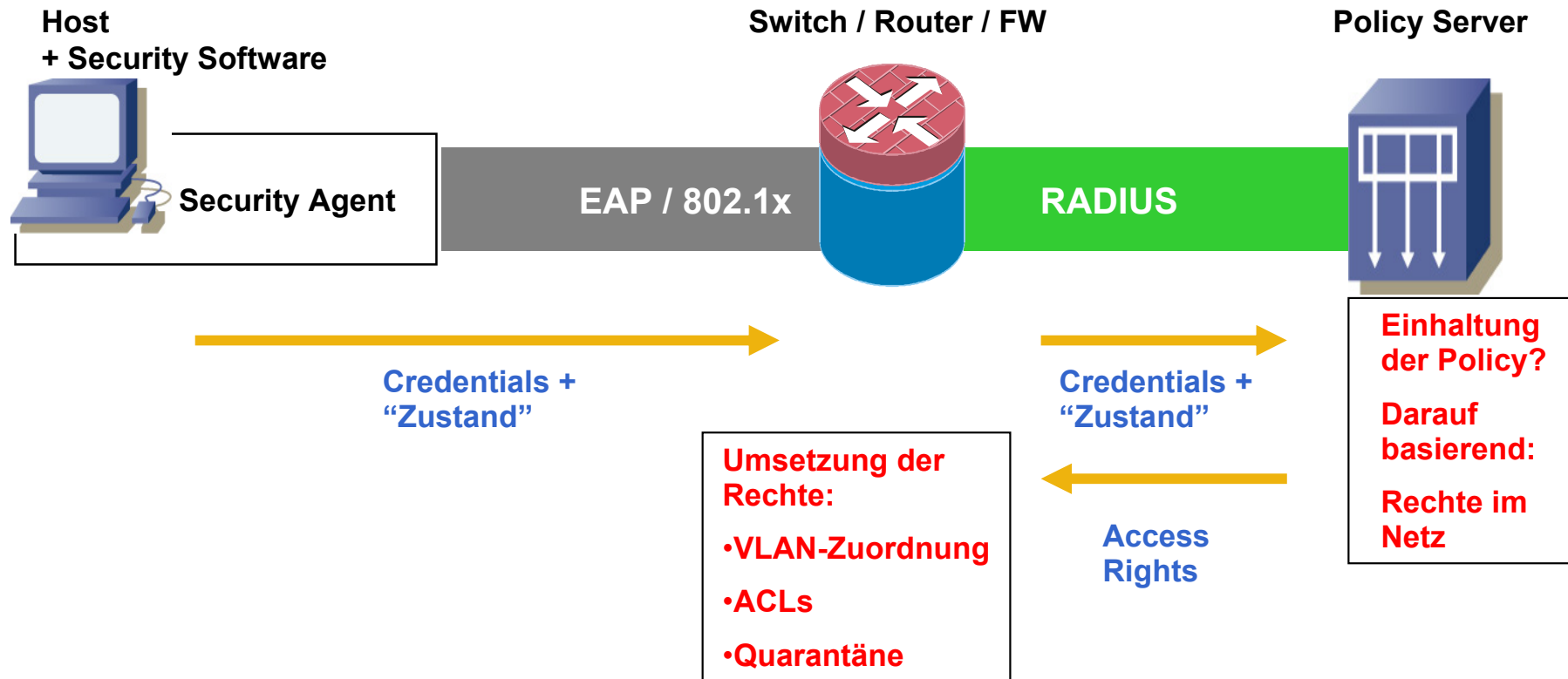
„Cisco Network Access Control“ (NAC)



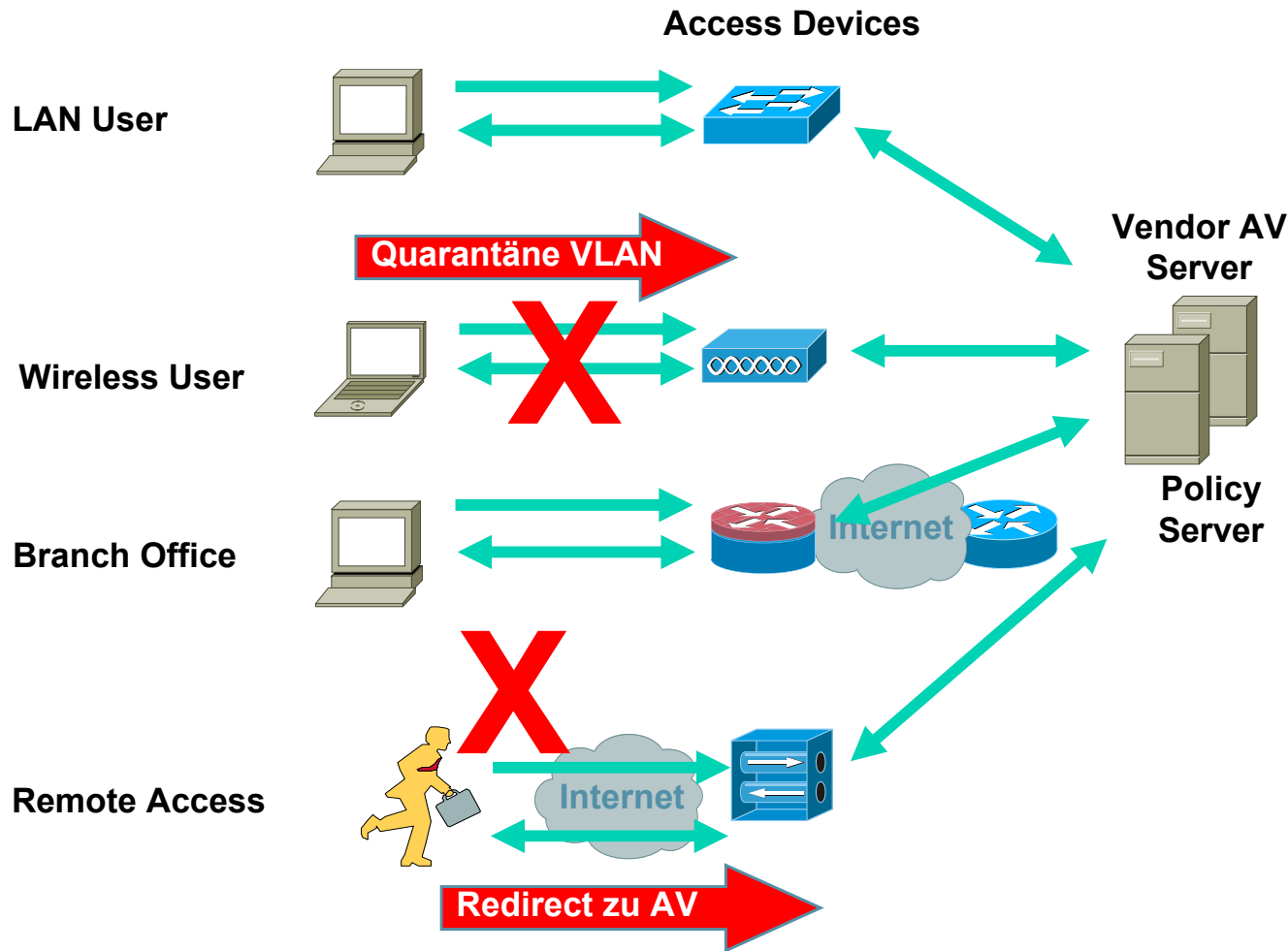
“Alter Hut”: 802.1X Authentifizierung im WLAN



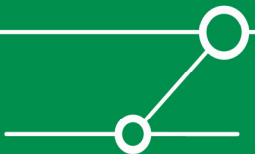
Kommunikationsschema: Policy basierte Zugangskontrolle



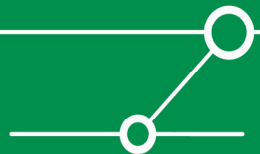
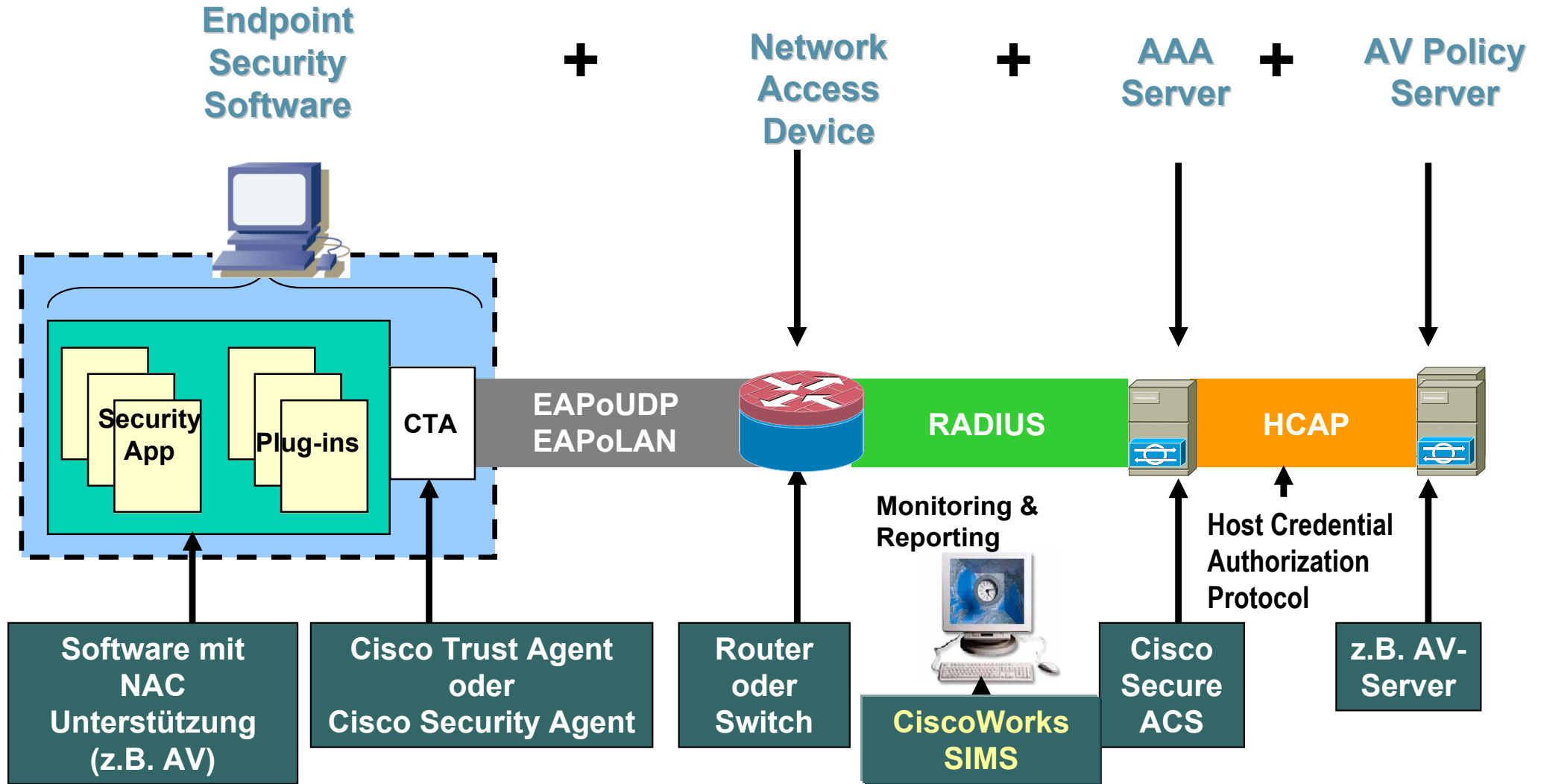
Policy-basierte Zugangskontrolle



1. Neue L2 oder L3 Verbindung durch Access Device festgestellt
2. Access Devices "befragt" Security Agenten auf dem Endpunkt
3. Policy Server vergleicht Information mit Policy. Entscheidung (OK, Deny, Quarantäne)
4. Access Device setzt Entscheidung um

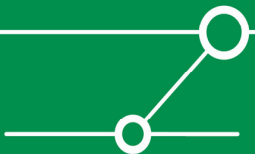


Cisco NAC Komponenten

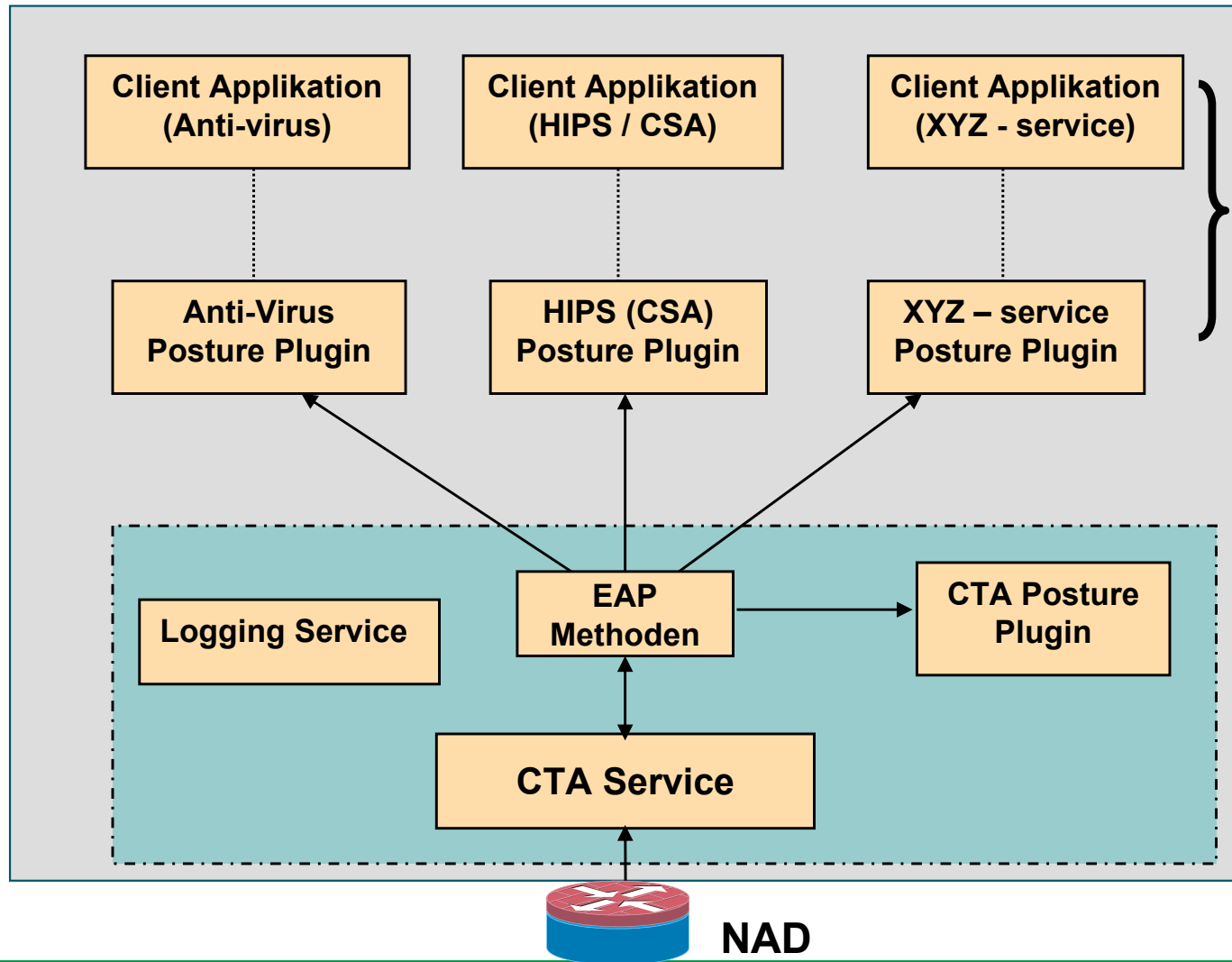


Cisco Trust Agent (CTA)

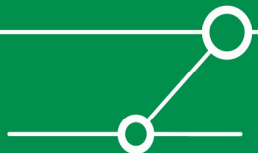
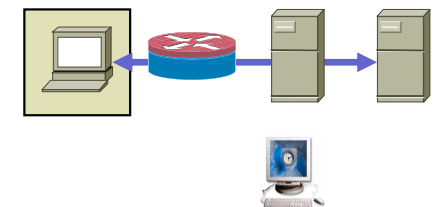
- Cisco Trust Agent
 - Software, die auf dem Endpunkt installiert wird und die Kommunikation mit dem Network Access Device durchführt (EAPoUDP, EAPoLAN).
 - Antwortet auf Anfragen von Network Access Devices mit Endpunkt Security Credentials.
 - Sammelt Security Zustandsinformationen von Endpunkt Security Software (AV, CSA, etc.).
 - Elementarer Bestandteil von Cisco Network Access Control (NAC).
 - Wird gebündelt mit unterstützter AV Software (z.B. TrendMicro OfficeScan Enterprise, McAfee Virus-Scan / ePO).
 - Initialer Fokus: AntiVirus



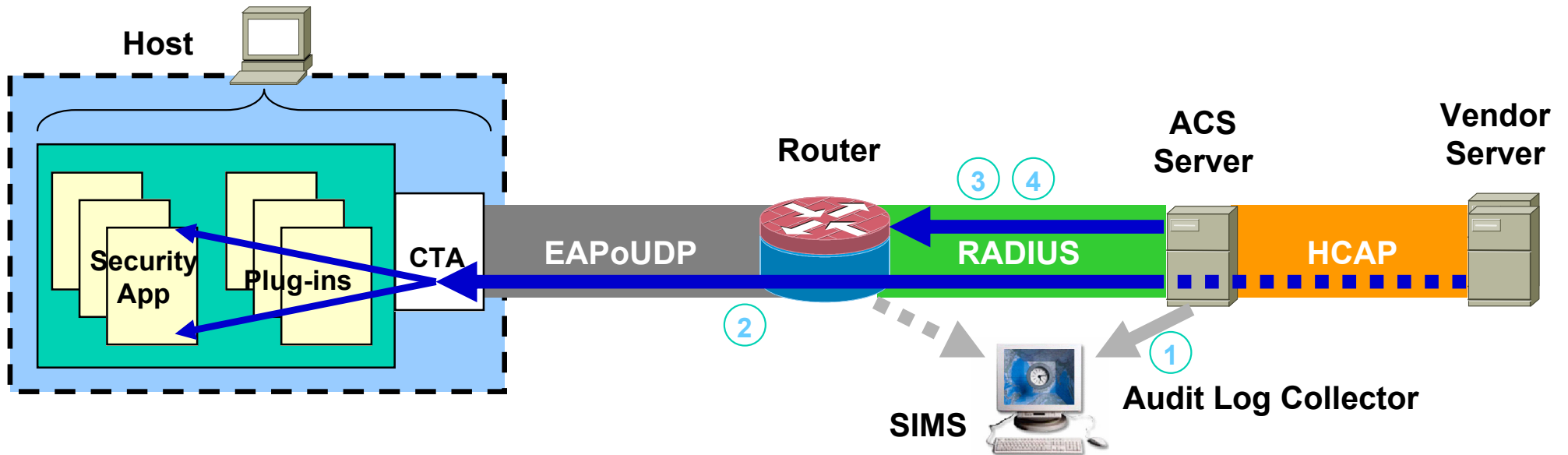
CTA: Architektur & Komponenten



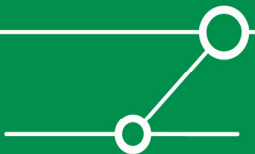
Für jede Applikation, die über sog. "Posture-Plugins" Zustandsinformationen mittels des CTA überträgt, muß ein entsprechender Policy Server vorhanden sein.



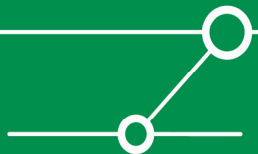
Posture Check Ergebnis



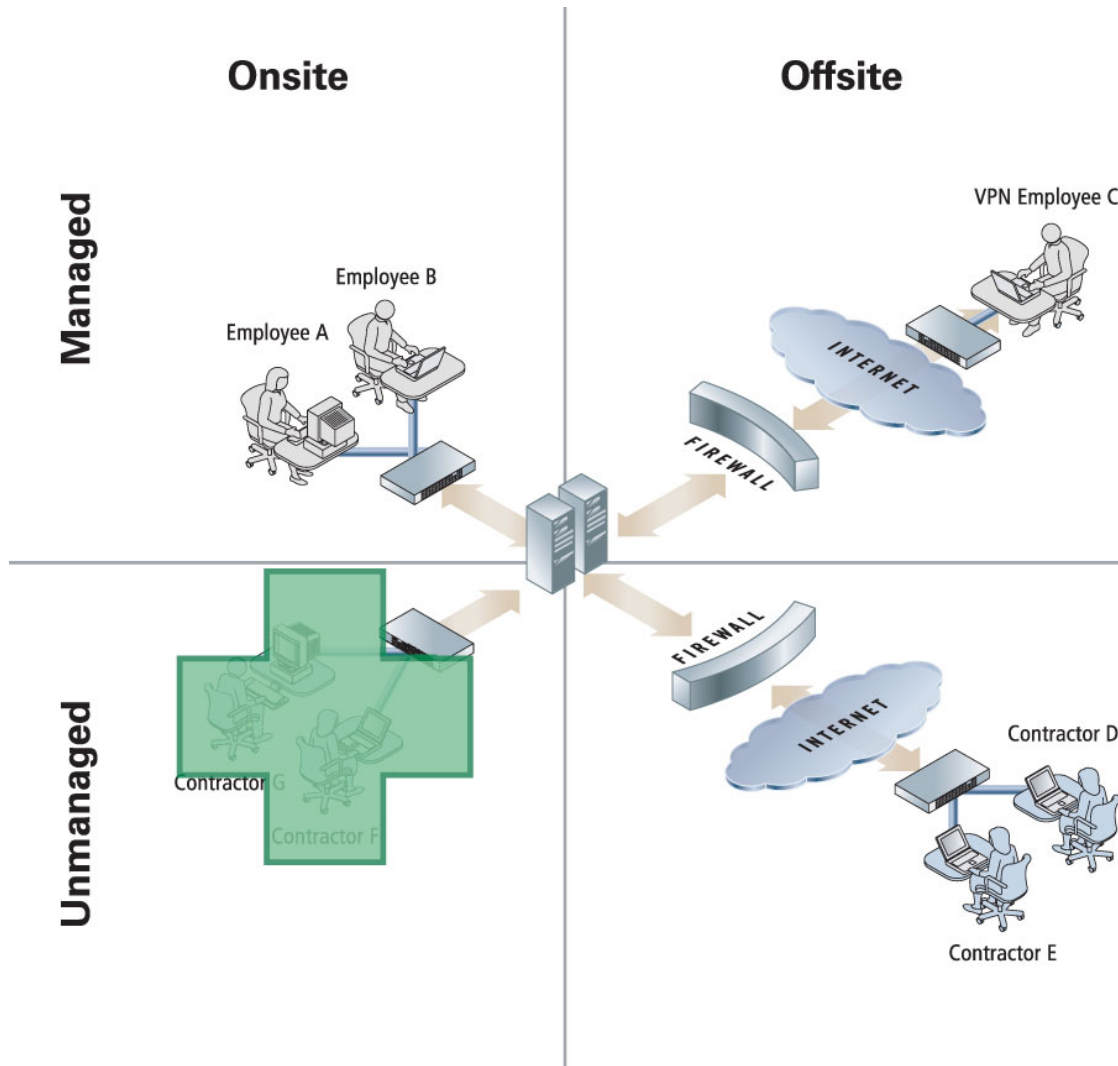
- Posture Check ergibt folgende Ergebnisse
 1. Audit logging für administrativen Feedback
 2. In-band Benachrichtigung für Applikationen & User
 3. Out-of-band User-Feedback per URL-Redirection
 4. Dynamische Autorisierung per ACLs
- Die ersten 3 Ergebnisse sind "Feedback Loops"
- Das letzte Ergebniss stellt den eigentlichen Zustand fest



Beispiel McAfee Policy Enforcer



McAfee Policy Enforcer – Funktionsweise



1. Definition

Define system compliance policies

2. Entdeckung

When new systems connect to the network

3. Untersuchung

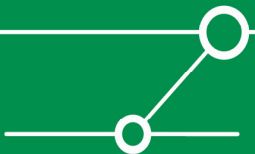
Real time assessment of compliance using network AND host-based tools

4. Umsetzung

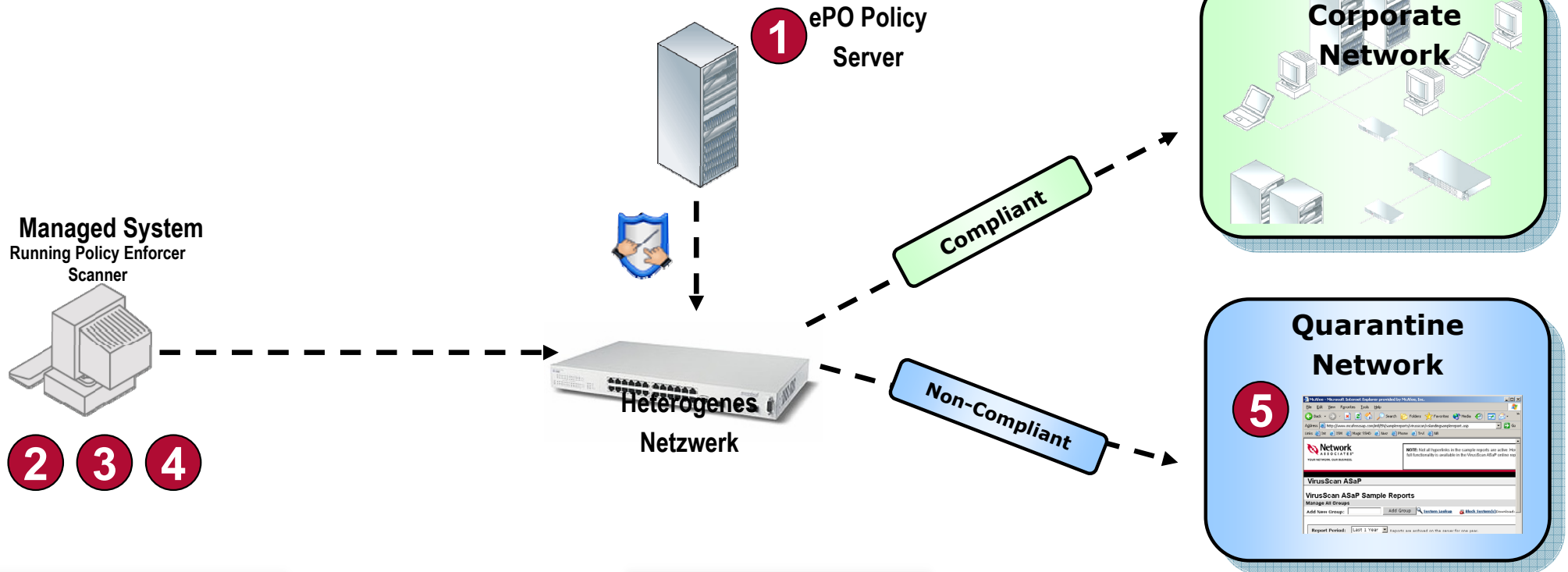
Non-compliant systems redirected to quarantine VLAN

5. Remediation

Non-compliant systems redirected to remediation portal



Self-Enforcement for Managed Systems



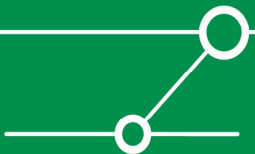
1 Define
Define system compliance policies

2 Detect
Policy Enforcer Scanner locally detects when the system connects to the network.

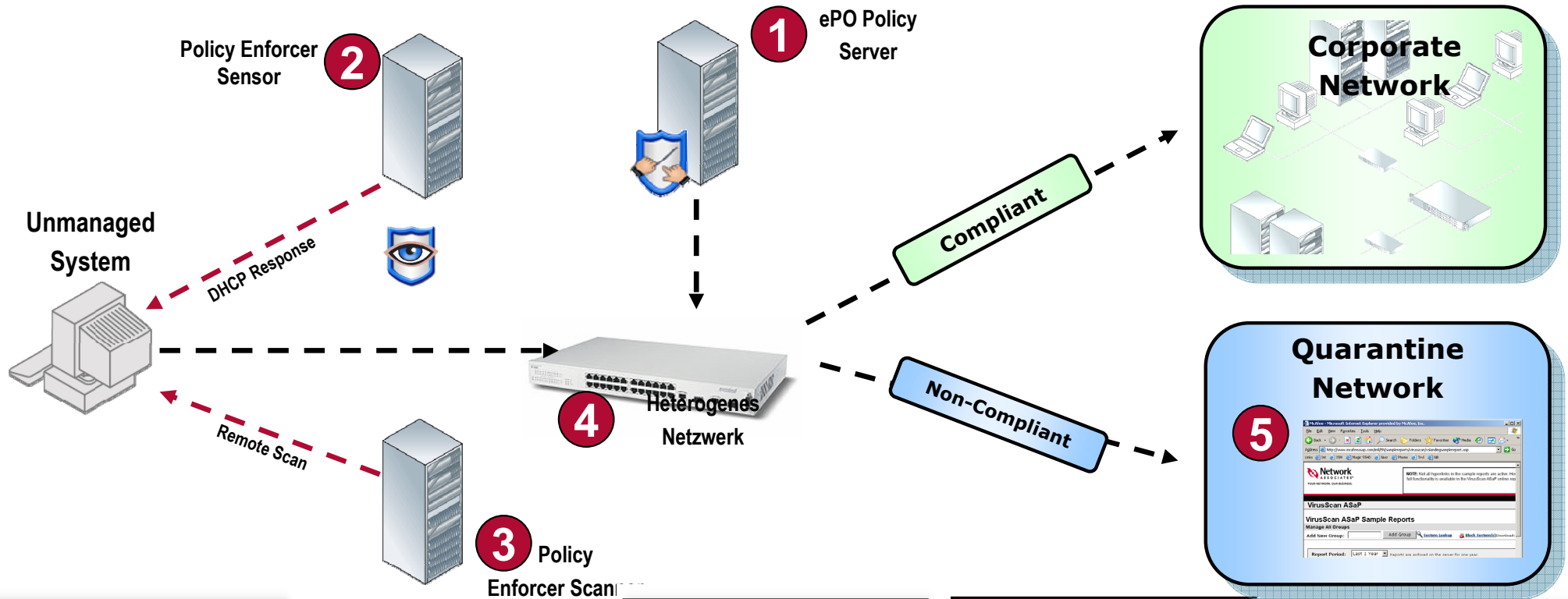
3 Assess
Before allowing access, Policy Enforcer Scanner scans the local system

4 Enforce
Non-compliant system is restricted to only accessing servers defined in the white list

5 Remediate
Non-compliant system connects to servers defined in the white list and takes necessary actions to remediate

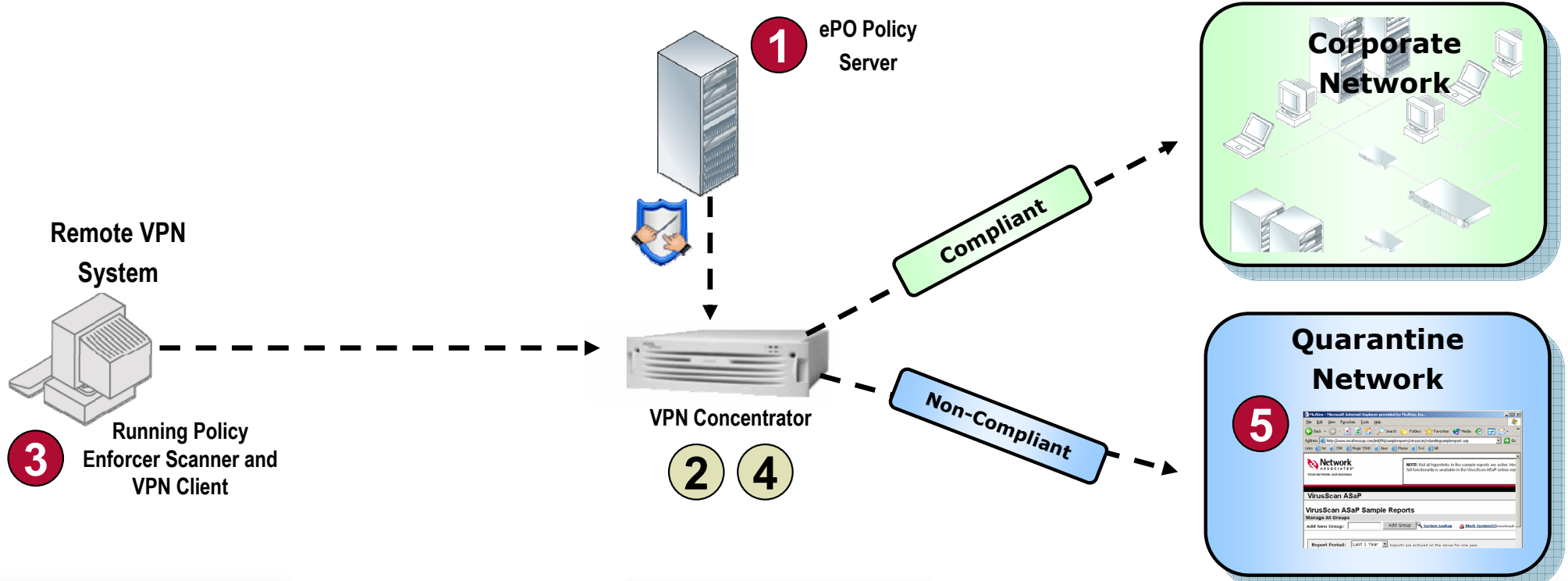


Switch-enforcement for Unmanaged Systems

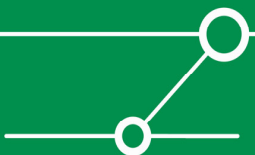


- | | | | | |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <p>1 Define</p> <p>Define system compliance policies</p> | <p>2 Detect</p> <p>Policy Enforcer Sensor detects when systems connect to the network (Broadcasts, ARP, DHCP)</p> | <p>3 Assess</p> <p>Policy Enforcer Scanner remotely scans for compliance</p> | <p>4 Enforce</p> <p>Non-compliant systems are redirected to Quarantine VLAN</p> | <p>5 Remediate</p> <p>Non-compliant systems redirected to Remediation Portal</p> |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|

Remote Access VPN Enforcement



- 1 Define**
Define system compliance policies
- 2 Detect**
Detect when new systems connect to the VPN concentrator
- 3 Assess**
Assess compliance using Policy Enforcer Scanner
- 4 Enforce**
Non-compliant systems limited to resources defined in the VPN network restricted access policy
- 5 Remediate**
Non-compliant systems redirected to Remediation Portal



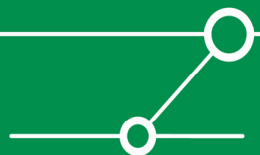
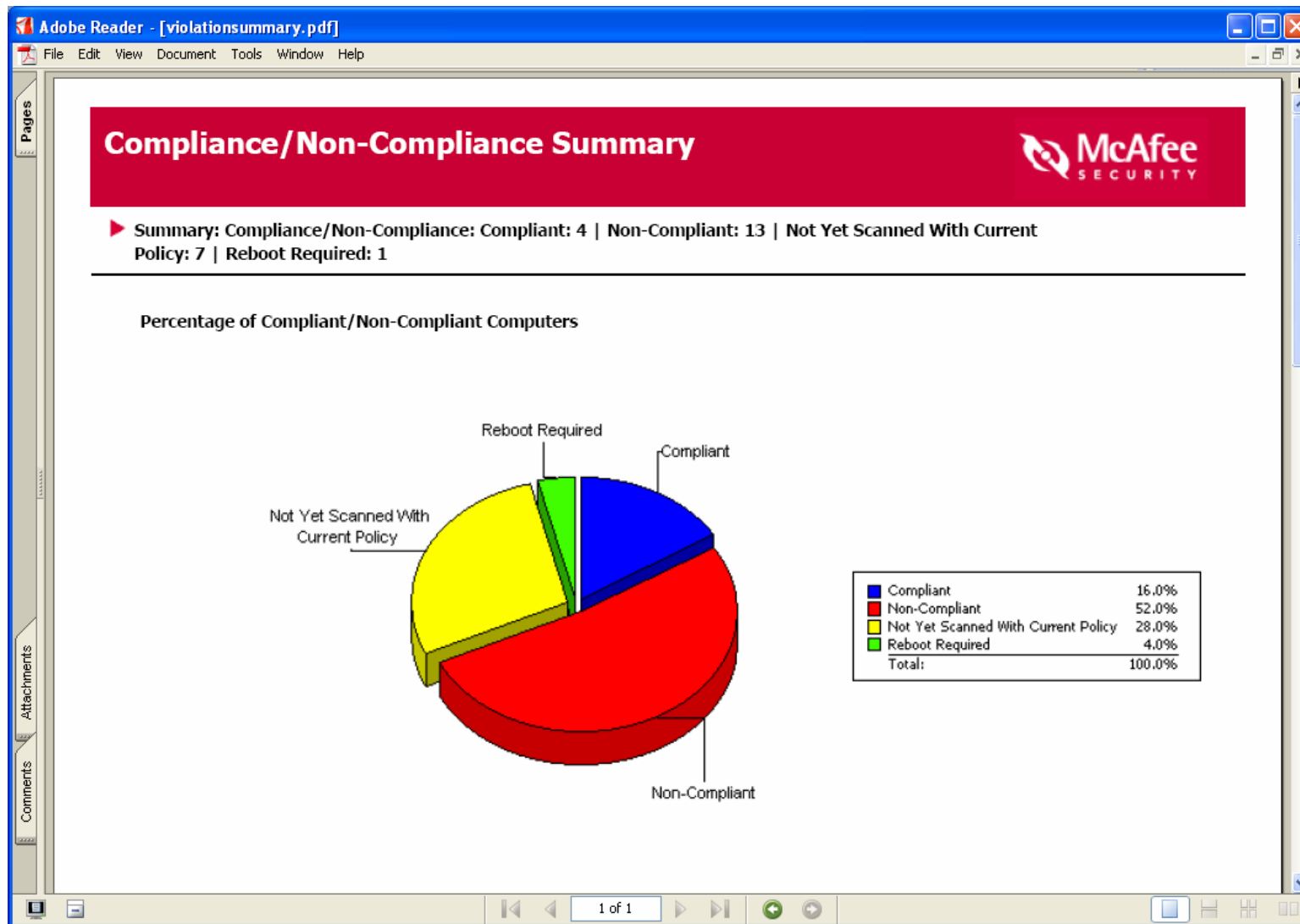
Beispiel McAfee: Compliance Profiler Policy

The screenshot displays the ePolicy Orchestrator 3.5 interface. On the left, a tree view shows the hierarchy: McAfee Security > ePolicy Orchestrator Agent > System Compliance Profiler 1.1. A red circle highlights the 'System Compliance Profiler 1.1' folder. The main window shows the configuration for this policy, including an 'Apply' button, the McAfee logo, and a list of rules. The 'Rules' section is expanded to show 'Security Patch Rules' with a list of specific rules and their QIDs. The 'Inherit' checkbox is unchecked. The 'Last Modified' date is Tuesday, January 24, 2006 10:58:24 AM. The 'Rules' list includes:

- Custom Rules
 - Windows OS Patches
 - Services
 - Security Patch Rules
 - MS01-034 (Q288266)
 - MS01-034 (Q302294)
 - MS01-038 (Q303825)
 - MS01-038 (Q303833)
 - MS01-055 (Q312461)
 - MS01-056 (Q308567)

Buttons for 'Add Rule', 'Add Group', 'Edit', 'Delete', 'Enable', 'Archive', 'Filter', and 'Advanced View' are visible on the right side of the rules list.

Beispiel McAfee: Compliance Profiler Report



Beispiel McAfee: Compliance Profiler Report

Compliance/Non-Compliance Summary
Computer Details

DRILLDOWN PATH: Compliance Details: Non-Compliant > Computer Details:

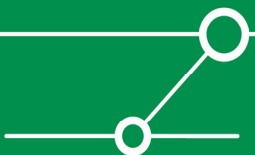
Computer Name	IP Address	Violation Count
DEH...	10.32.1...	5

Computer Details

Directory	Operating System	Platform	Version	MAC Address
DEH...	Windows 2000	Workstation	5.0	...

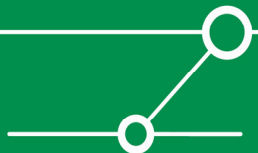
Group Details
Drill down for more details by selecting a group row

Group Directory Path	Rules Violated
MS01-034 (Q288266)\Patch 1: Word \Patch Details	1
MS01-034 (Q288266)\Patch 1: Word \Word\Word 2000	1
MS03-023 (Q823559)\Patch 3: 2000 \Patch Details	2
MS03-023 (Q823559)\Patch 3: 2000 \Service Packs	8
MS03-035 (Q827653)\Patch 1: Works Word Office \Office\Office 2000	1
MS03-035 (Q827653)\Patch 1: Works Word Office \Patch Details	1



Kurzüberblick über weitere Frameworks

Framework / Organisation	Bemerkung & Produkte
Microsoft Network Access Protection (NAP)	Angekündigt für Vista & Longhorn. Wahrscheinlich hoher Durchdringungsgrad. Details derzeit nicht bekannt
Trusted Computing Group (TCG) Trusted Network Connect (TNC)	Offenes Framework, von vielen Herstellern Unterstützung angekündigt. Derzeit kein Produkt.
Checkpoint Total Access Protection (TAP)	Integrity Produktpalette seit ca. 3 Jahren auf dem Markt. Basiert auf IEEE 802.1x bzw. EAP (also offenen Standards).
...	...



Vielen Dank für Ihre Aufmerksamkeit

Fragen?

...

Und Antworten!

