infraray

Network Security Management

für IT und industrielle Netzwerke

Überwachen, steuern und sichern Sie alle Switches,
Router, Gateways, Server, Ports und Endgeräte.

www.infraray.com

Inhalt

Zweck dieses Dokuments

Dieses Dokument ist eine Einführung in die Sicherheits-funktionen der Infraray Business Infrastructure Control Solution (BICS) für IT- und industrielle Steuerungsnetzwerke.

Es vermittelt potenziellen BICS-Kunden ein Verständnis für die ganzheitliche Integration, den Lösungsansatz und die Fähigkeiten von BICS, einschließlich der Funktionen, die für BICS einzigartig sind.

Dieses Dokument ist kein Tutorial und ersetzt nicht die technische Dokumentation des BICS. Wir empfehlen Interessenten, sich mit Infraray in Verbindung zu setzen, um eine Live-Demonstration über das Internet zu vereinbaren. Eine ausführliche Live-Demonstration wird empfohlen. Bitte kontaktieren Sie Infraray, um eine Präsentation und Fragen und Antworten für Ihr Team zu vereinbaren.

BICS Network Security Management für IT & Industrienetzwerke

BICS for IT Security und sein Pendant, BICS für Industriesicherheit, meistern zentrale Herausforderungen bei der Absicherung komplexer, heterogener IT- und industrieller Steuerungsnetzwerke. BICS ermöglicht die Erkennung, Überwachung und Steuerung von IT- und industriellen Netzwerk-Endgeräten und die Fähigkeit, mit deren Befehlssätzen zu "sprechen".

Überwachen, steuern und sichern Sie alle Switches, Router, Gateways, Server, Ports und Endgeräte.

Aus Gründen der Einfachheit und Kürze wird in diesem Dokument auf die Infraray Business Infrastructure Control Solution (BICS) als "BICS for IT Security" oder "BICS for Industrial Security" oder "Infraray BICS for Security" oder einfach "BICS" verwiesen. Bitte beachten Sie, dass Infraray BICS eine umfassende Plattform ist, die neben Security weitere Module für Asset Management, Network Monitoring und eine Reihe weiterer wichtiger Unternehmensnetzwerkfunktionen enthalten kann.

Infraray BICS kann das Netzwerk zentral überwachen, steuern und sichern, Switches und Gateways in einer heterogenen Infrastruktur (sowohl für die IT- als auch für die Betriebsinfrastruktur) automatisch abfragen und verbundene Endpunkte, Ports und Uplinks identifizieren. Da seine Erkennung,

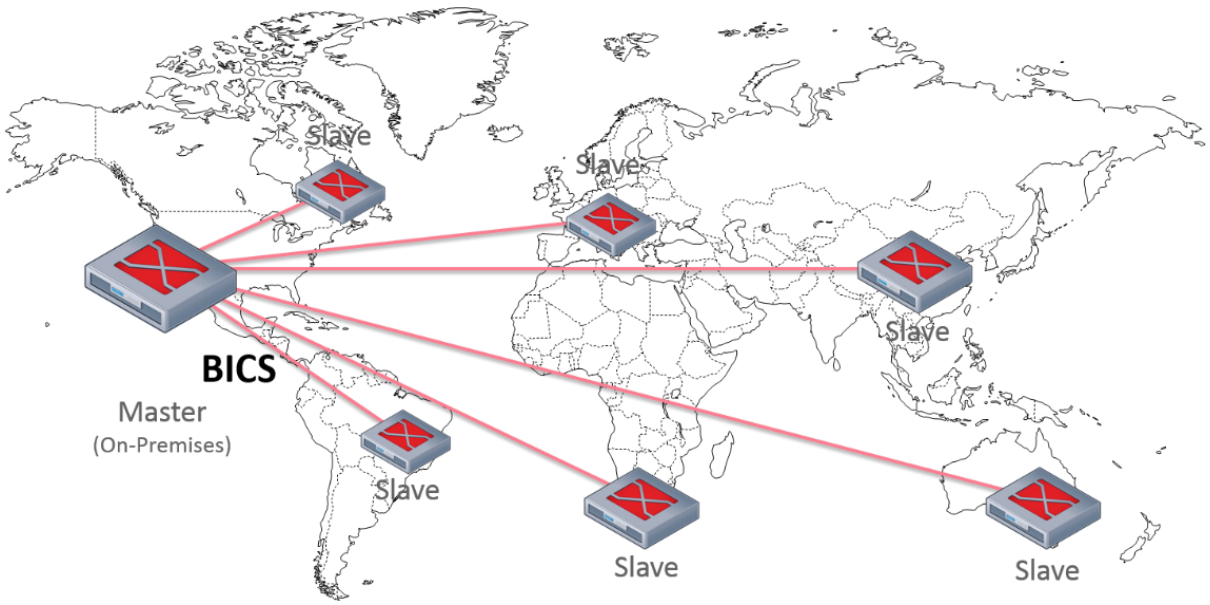
Überwachung und Steuerung umfassend ist und mit Tausenden von Gerätetypen, Marken und Modellen kommunizieren kann, unterstützt BICS die Herstellerunabhängigkeit und Geräteheterogenität.

Zur Verwaltung der Network Security für industrielle Netzwerke verwenden die Betreiber der BICS-Plattform Schnittstellen und Bildschirme, die mit denen in BICS identisch sind, um IT-Netzwerke zu verwalten.

1. Skalierbarkeit, Master-Slave-Architektur, Mandantenfähigkeit

- Die Funktionen von BICS lassen sich auf Netzwerke mit einer Million oder mehr Ports oder angeschlossenen Endpunkten sowie auf über 4.000 Mieter-Netzwerke im Mandantenmodus skalieren.

- BICS bietet eine Master-Slave-Architektur an (Multi-Instanz-Modus). Informationen etwa für den geographischen Raum „Südamerika“ etwa laufen in einer „Slave“-Instanz zusammen. Somit wird eine hohe Performanz dieser Instanz sichergestellt, da dort nur jene Informationen verarbeiten werden, die dieser Instanz zugeordnet sind (hier: Zuordnung auf Basis geografischen Kriteriums). Gleichzeitig werden alle Daten in der „MASTER“-Instanz konsolidiert – hier steht also der Gesamtüberblick über das Unternehmen zur Verfügung.



2. BICS Network Security Management Features

- Verifizierung und Verwaltung von Netzwerkgeräten und Ports für die Steuerung, Verwaltung und Sicherheit von Informationstechnologie (IT) und Betriebstechnik (OT).
- Unterstützt IEEE 802.1X, MAC und PWA Authentifizierung.
- Herstellerunabhängige NAC-Lösung.
- Entwickelt für die Absicherung heterogener Netzwerke jeder Größe, von mittelgroß bis sehr groß, einschließlich solcher mit Hunderttausenden von Endpunkten.
- Single-Pane-Of-Glass, intuitive Benutzeroberfläche für zentrale Überwachung und Steuerung. Visuelle Darstellung der gesamten Netzwerkinfrastruktur mit topologischen, geographischen und organisatorischen Ansichten in Echtzeit / dynamisch. Drilldown vom High-Level-Dashboard zum diskreten Endpunkt.
- Automatische Erkennung und punktgenaue Lokalisierung, einschließlich Alarm und Warnungen.
- Analyse der Datenflüsse im gesamten Netzwerk.
- Schnittstellen zur Integration vorhandener Sicherheitssoftware (z.B. Splunk).

3. Key BICS-Aufgaben für Network Security Management Control

Identifizieren Sie Geräte über MAC Layer 2 eindeutig und weisen Sie diesen Geräten automatisch Rollen zu. Wenn das Gerät IEEE 802.1X unterstützt, kann BICS auch den Endbenutzer identifizieren und spezifische

Berechtigungen identifizieren, die jeder Benutzer besitzt wie VLAN-Berechtigungen und -Einschränkungen.

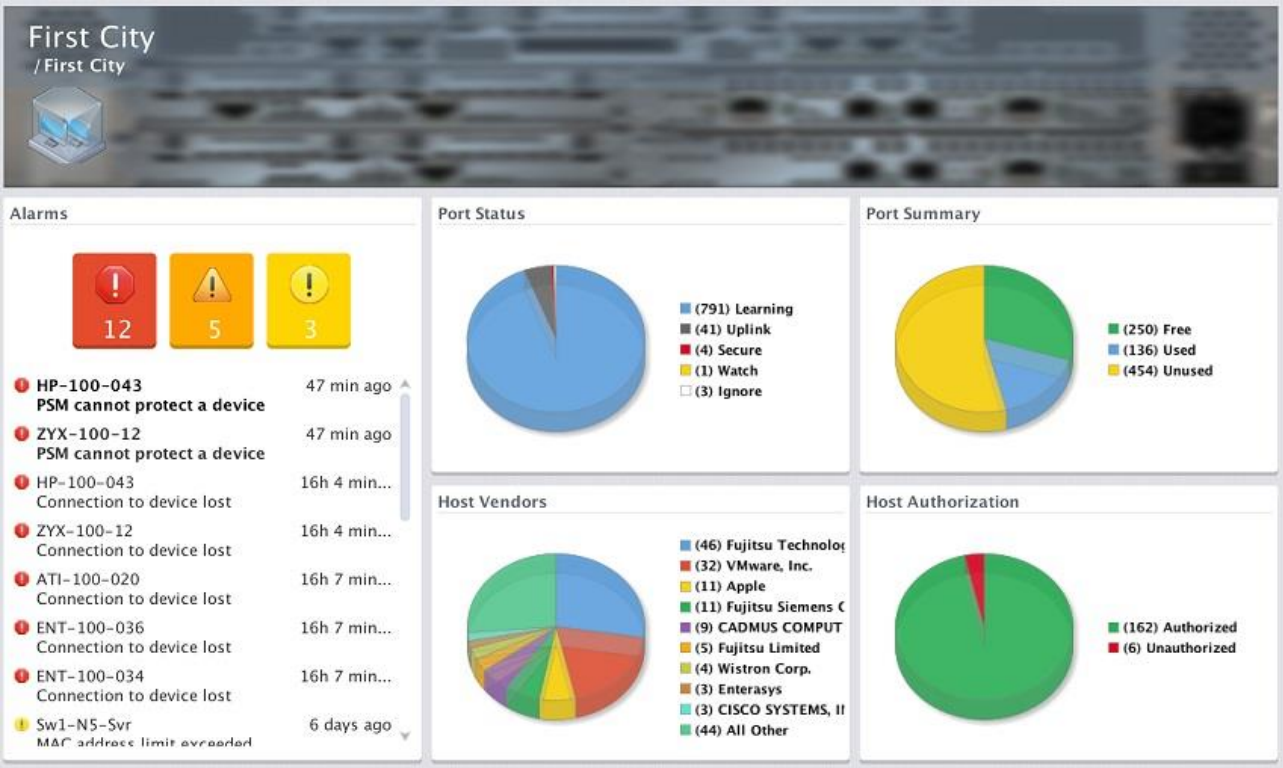


Abb. 1 Grafisches Dashboard mit granularen Alarm-Updates und aktuellen Zusammenfassungen des Port-Status

Mit der Implementierung von 802.1X ermöglicht der BICS Policy Editor die Verwaltung und Vorbereitung individueller Richtlinien und Rollen für verschiedene Benutzer- oder Gerätegruppen.

BICS for Security bietet weniger detaillierte Richtlinieneinstellungen in MAC Layer 2 Implementierungen.

- Automatische Einhaltung von Sicherheitsanforderungen, z.B. White List, 802.1x-Zertifikat
- Erzwingen Sie festgelegte Sicherheitsanforderungen in Echtzeit, wie z.B. das Einschränken oder vollständige Blockieren eines unbekannten Geräts für den Zugriff auf das Netzwerk.
- Erkennen und melden Sie den Verbindungsstandort, den Port und den Switch, die von jedem Endpunkt verwendet werden.
- Geben Sie bei Bedarf Alarme aus.

INFRARAY BICS for Security teilt die erfolgreiche Leistung des Port Security Managements in die folgenden Schritte auf:

2.1 Erkennung, Lokalisierung und Authentifizierung

BICS erkennt und lokalisiert automatisch den Switch- und Port-Verbindungspunkt jeder Netzwerkkomponente in Echtzeit, einschließlich

drahtloser Netzwerke (WLANs). Diese Funktionalität ist unabhängig vom Ort des Zugriffs.

BICS ermöglicht die eindeutige Authentifizierung von Benutzern und Geräten zur Gewährleistung der Identität jedes einzelnen gemäß dem IEEE 802.1X-Standard.

2.2 Assessment

BICS prüft, ob die MAC-Adresse, der Benutzername (bezogen auf 802.1x), das Passwort und/oder das Zertifikat während des Anmeldevorgangs in Echtzeit gültig sind.

2.3 Autorisierung

- Zugriffskontrolle für Benutzer und Geräte, wobei der Zugriff auf Bereiche, die durch Sicherheitsanforderungen definiert sind (Gast-, Quarantäne- oder Produktionsbereiche), auf der Grundlage der vorhergehenden Prüfungen korrekt gewährt wird.

- Automatisches Alarmverfahren bei unberechtigtem Netzwerkzugriff oder fehlerhaftem oder verdächtigem Verhalten eines Endgerätes.

- Reaktion in Echtzeit: BICS kann ein Gerät sofort und automatisch vom Netzwerk trennen und - wenn die Richtlinie dies vorsieht - innerhalb eines Gastnetzes isolieren.

Abb.2: Beispiel für ein "CIO" Single-Pane-of-Glass Dashboard in BICS

2.4 Single-Pane-of-Glass Monitoring und Kontrolle

Single-Pane-of-Glass ist die vereinfachte, intuitive Benutzeroberfläche zur zentralen Überwachung und Steuerung von Netzwerken und Endgeräten.

(i) Visuelle Darstellung der gesamten Netzinfrastruktur.

(ii) Echtzeit / dynamischer Drill-Down vom High-Level-Dashboard zum diskreten Endpunkt.

(iii) Anpassbare Ansichten basierend auf Rollen oder Unternehmens-richtlinien.

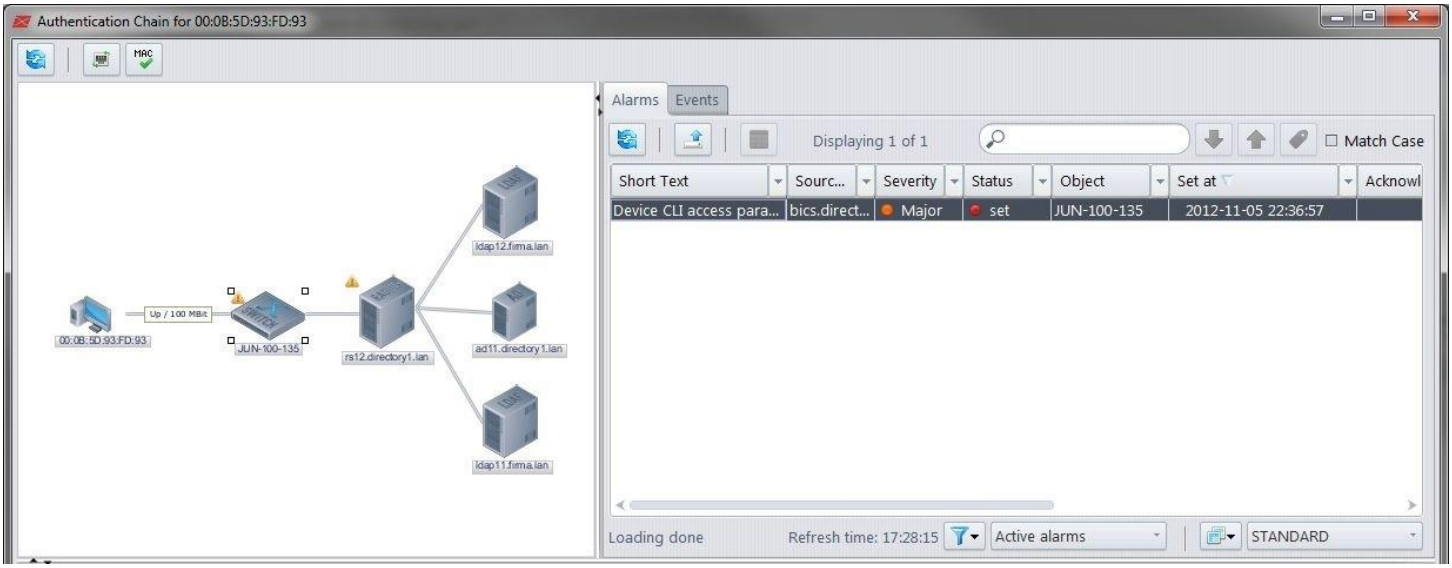


Abb. 3 BICS zeigt die Sicherheitsauthentifizierungskette für jedes Gerät im Netzwerk an.

BICS for Security kann auch die Authentifizierungskette eines beliebigen Endpunktes in der IT- oder OT-verknüpften Infrastruktur in Echtzeit abbilden.

Single-Day: Die eintägige Einführung kann die Anforderungen von Imminent-Bedrohungsszenarien erfüllen.

BICS for Security kann sehr schnell eingesetzt und implementiert werden. Bei MAC Layer 2 Implementierungen kann dies schon nach wenigen Stunden der Fall sein. Dies kann in einer drohenden Gefahrensituation wichtig sein. Die für 802.1X-Implementierungen benötigte Zeit ist bei BICS for Security schneller als bei Konkurrenzprodukten und hängt von Faktoren wie Kundenanforderungen, Übersichtlichkeit und Komplexität der Netzwerkstruktur und anderen konfigurationsbedingten Problemen ab.

Einmal implementiert, kann BICS innerhalb eines Tages Hunderttausende von Ports entdecken und diese ständig überwachen. Es bietet eine automatisierte, vollständige Virtualisierung ganzer IT-Umgebungen bis auf Port-Ebene und zeigt den physischen Zustand und Zustand jedes Geräts an.

Zusätzlich zu den Geräten, die BICS in einem IT-Netzwerk entdeckt und steuert - Cisco, HP, Dell, Extreme und andere gängige Gerätemarken - in industriellen OT-Netzwerken, entdeckt und erkennt BICS auch IP-adressierbare Industriegeräte, Gerätemarken und Modelle: MOXA, Phoenix, Hirschmann, Siemens, Belden, Schneider und zugehörige Endgeräte.

Wie bei IT-Netzwerken kommuniziert BICS mit diesen Industriegeräten in ihren nativen Befehlssätzen. BICS stellt dem Anwender einen gemeinsamen Satz von BICS-Befehlen zur Verfügung, um Gruppen von Geräten und/oder einzelne Geräte von einer zentralen Stelle aus zu steuern.

3. Network-Port Security Management

Network Security wird in INFRARAY BICS for Security als Schlüsselkomponente namens Port Security Management ausgeliefert. Es ermöglicht die Netzwerkzugriffskontrolle für Unternehmen jeder Größe und für mehrere Einheiten.

BICS ermöglicht Sicherheit für jeden Netzwerk Port, indem es über den zugehörigen Ethernet-Switch arbeitet und jede Port-Schnittstelle permanent mit einer oder mehreren MAC-Adressen verknüpft. Die Geräte mit diesen MAC-Adressen sind auf die Kommunikation mit dem Netzwerk über diese Schnittstelle beschränkt, wodurch der Zugriff auf das Netzwerk durch nicht autorisierte Endgeräte verhindert und bestimmte Angriffe aus dem eigenen Netzwerk blockiert werden.

Darüber hinaus unterstützt Infraray BICS den Standard IEEE 802.1X, um die Netzwerk-Port-Sicherheit weiter zu erhöhen. Anstatt die MAC-Adresse am Port zu "kleben" (wie wenn 802.1X nicht möglich ist), wird sie auf einem RADIUS-Server gespeichert und von 802.1X angesprochen. Die IEEE 802.1X-Authentifizierung ermöglicht die weltweite Verwaltung einer MAC-Adresse in einem LAN oder VLAN und unterstützt eine hohe Benutzermobilität.

Infraray BICS managed die Sicherheit für Netzwerk-Ports

Die Netzwerk-Port-Sicherheit von Infraray BICS kann automatisch erkennen, ob ein Benutzer, der versucht, sich anzumelden, die richtige Berechtigung von dem ihm zugewiesenen System oder Gerät hat. Wenn diese Parameter übereinstimmen und den Anforderungen entsprechen, erhält der Anwender - im Rahmen der ihm gewährten Zugriffsrechte (Voraussetzung: IEEE 802.1X, User Certificates, VLAN-Steuerung) - Zugriff auf Unternehmensressourcen. Versucht ein Benutzer, sich unberechtigt anzumelden, löst BICS automatisch einen Alarm aus und verhält sich entsprechend den voreingestellten Sicherheitsrichtlinien - zum Beispiel durch automatische Sperrung des Ports.

4. Device Control Bibliothek und Herstellerunabhängigkeit

Infraray ermöglicht Herstellerunabhängigkeit für eine umfassende Netzwerksicherheit. Cisco, HP, Allied Telesis, Nortel, Juniper, Dell und Enterasys gehören zu der langen Liste von Herstellern, die BICS auf Befehlszeilenebene überwachen und steuern kann, um IT-Netzwerke zu

verwalten, zu kontrollieren und zu sichern. Für industrielle Netzwerke überwacht und steuert BICS eine breite Palette von Geräten der Hersteller MOXA, Phoenix, Hirschmann, Siemens, Belden, Schneider und zugehörige Endpunktgeräte.

Die Infraray BICS Device Control Library ist umfangreich und macht BICS effektiv herstellerunabhängig. Mit BICS wird es ermöglicht, das Netzwerk-management und Port Security Management für das gesamte Netzwerk abzudecken, auch wenn es Geräte von zahlreichen verschiedenen Herstellern enthält. Das Einbinden eines neuen Gerätes in die Device Control Bibliothek dauert in der Regel ca. drei Tage - schnell durchgeführt von einem dedizierten Integrationsteam.

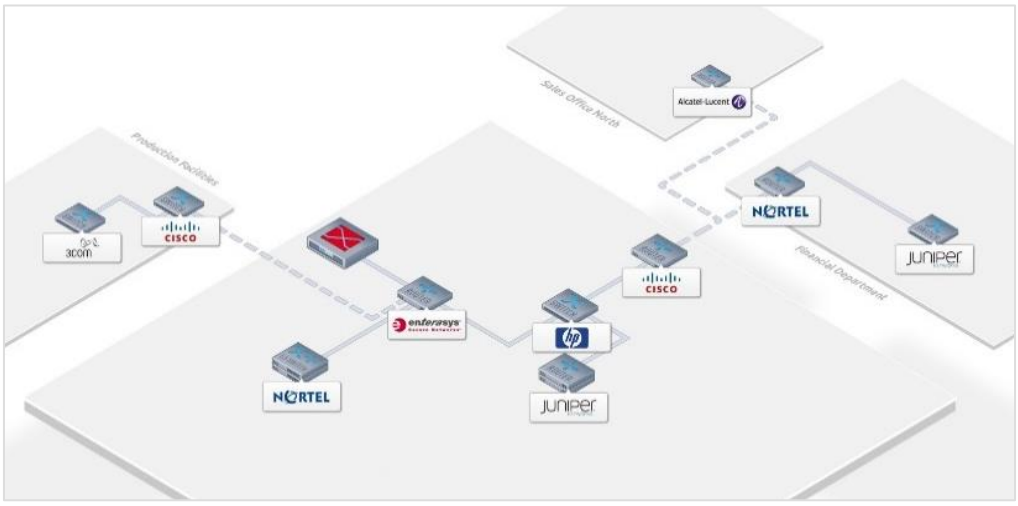


Abb. 4 Die Infraray Device Control Library ermöglicht volle Herstellerunabhängigkeit. Die Integration eines neuen Netzwerkgerätes in die Device Control Library dauert in der Regel zwei Tage.

5. Unbefugten Zugriff auf das Netzwerk blockieren

BICS ermöglicht es Netzwerk-Switches, den unerwünschten LAN-Zugriff durch nicht autorisierte Endgeräte zu blockieren und regelt die Sicherheitseinstellungen der einzelnen Geräte und Ports.

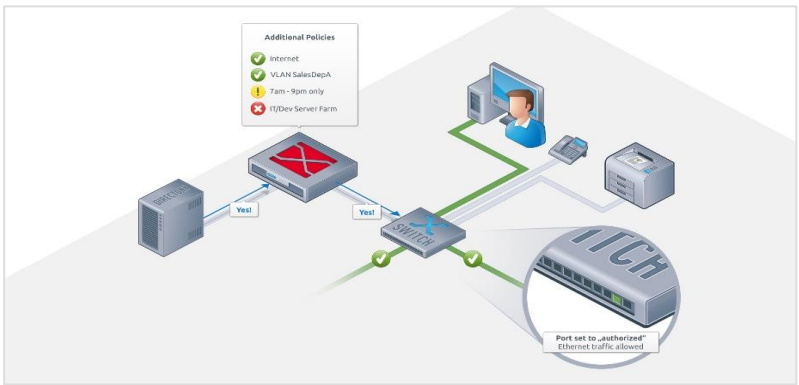


Abb 5 BICS ermöglicht die automatische Steuerung aller Ports, Gruppen von Ports und einzelner Ports.

5.1 Feature Description

- **BICS sichert das LAN, um den Anschluss unbekannter Geräte zu verhindern.**
  Nur Geräte mit bekannten MAC-Adressen, die auf einer Whitelist gespeichert sind, dürfen das LAN nutzen. BICS gibt einen Alarm an einen bestimmten Betreiber aus und / oder schaltet jeden Port ab, auf den ein unbekanntes MAC adressiertes Gerät zugreifen will.

- **Überprüft (im Lernmodus) das Netzwerk, um festzustellen, welche MAC-Adressen von jedem angeschlossenen Endgerät verwendet werden.**
  BICS erkennt die angeschlossenen Endpunkte und speichert deren MAC-Adresse in der Infraray BICS-Datenbank (CMDB).

- **Erkennt und speichert die Verbindungszeit und den Portstandort für jeden Endpunkt.**
  BICS pflegt und aktualisiert ständig eine Datenbank mit der Verbindungs-historie jedes Endpunktes.

- **Überwacht (Events & Alarme) Endpunkt-Verbindungsereignisse und Gerätebewegungen von Port zu Port im Netzwerk.**
  Jede erfolgreiche und erfolglose Verbindung wird in der BICS-Datenbank der Verbindungshistorie gespeichert.

- **Erkennt MAC-Spoofing.**
  BICS gibt Alarm, wenn der Verdacht auf doppelte MAC-Adressen und neue MAC-Adressen besteht, die über mehrere Ports zugreifen.

- **Verhindert die Verwendung von MAC-Adressen an verschiedenen Orten oder gegen die Sicherheitsrichtlinien.**
  BICS ermöglicht es dem Betreiber, eine beliebige MAC-Adresse oder eine Gruppe von MAC-Adressen an bestimmte Orte und Ports zu binden.

- **Hilft, blockierte Situationen zu lösen.**
  Gibt dem Netzbetreiber Vorschläge zur schnellen Lösung von Block-situationen**.**

Dieser Auszug aus einem BICS for Security-Bildschirm zeigt ein Beispiel für "Reparaturhinweise" und empfohlene Aktionen, die BICS dem Netzbetreiber im Falle eines Zugriffsfehlers für ein Gerät anzeigt.

Abb. 6 BICS for Security empfiehlt Korrekturmaßnahmen, die die Auswirkungen menschlicher Unterlassungen und Fehler reduzieren.

5.2 Kontrolle und Steuerung der Switches

BICS Configure setzt automatisch jeden erkannten Switch, der vom Infraray Netzwerk-Port-Sicherheitsmanagement gesteuert wird.

Der Bediener kann auch Schalter einzeln und in Gruppen für den Betrieb unter der Kontrolle von BICS bestimmen.

BICS erkennt die folgenden fünf Zustände für jeden Port und lässt sie vom Betreiber manuell oder automatisch an jedem Switch für jeden Port konfigurieren. Auf einem Switch, der unter BICS-Kontrolle steht, hat jeder Port immer einen der folgenden Zustände (aber nie mehr als einen):

- **Learn**: Lernt die MAC-Adresse und speichert sie in der BICS CMDB. Dies bedeutet, dass die MAC-Adresse autorisiert ist.
- **Secure**: Beendet sofort einen Port, an dem eine nicht autorisierte MAC-Adresse den Zugriff versucht, oder überschreibt andere Einstellungen und ordnet das Endgerät sofort einem Quarantäne-VLAN zu. Diese Aktion speichert auch die MAC-Adresse in einer "schwarzen Liste".
- **Watch**: Überwacht eine nicht autorisierte MAC-Adresse, speichert sie in einer schwarzen Liste und gibt einen Alarm aus, schaltet aber den Port nicht ab.

- **Uplink**: Ein automatischer Prozess, der den Port erkennt, wird als Uplink zu einem anderen Switch oder Router verwendet, nicht als Zugriffspunkt für ein Endgerät.

- **Ignore**: Der Operator kann einen Port als Ausnahme für diese Prozesse/Aktionen festlegen, indem er ihn in den Zustand Ignorieren versetzt.

Weitere Funktionen:

- Binden Sie Endpunkte an Ports.
- Die MAC-Adresse des Endpunkts kann an einen bestimmten Port gebunden werden.
- Definieren und überwachen Sie Sicherheitsereignisse und Alarme.
- Im BICS-Konfigurator kann der Bediener aus vordefinierten Alarmen auswählen und / oder neue Alarme definieren und hinzufügen.

6. IEEE 802.1X Unterstützung

Infraray BICS verwendet IEEE 802.1X und ermöglicht das Extensible Authentication Protocol. BICS verbessert die Verwaltung der geräte- und portbasierten Einstellungen dieser Authentifizierungsmethode und ermöglicht deren Einbindung in eine bestehende 802.1X-Struktur..

6.1 Feature Beschreibung

- **LAN gesichert, um die Verbindung von unbekannten Geräten (Gerätezertifikat) und Benutzern (Benutzerzertifikat) mit dem Netzwerk zu verhindern**.
  Wenn ein Antragsteller Zugriff auf das Netzwerk beantragt, verwaltet BICS den Autorisierungsprozess und legt die Zugriffsrechte auf die Netzwerkkomponente fest.

- **Sichern Sie das LAN für die Verwendung mit nicht unterstützenden Geräten mit MAC-Authentifizierungsbypass.**
  Diese Methode kann für nicht liefernde Geräte, wie z.B. Drucker, verwendet werden.

- **Sichern Sie das LAN mit Port Web-based Authentication (PWA) oder Captive Portal.**
  BICS kann diese gemeinsame Methode zur Verfügung stellen, um den Zugriff auf das LAN zu ermöglichen.

- **Stellen Sie fest, ob Netzwerkgeräte die IEEE 802.1X-Authentifizierungsmethode verwenden können.**

BICS überprüft das Gerät während des Erkennungsprozesses, um festzustellen, ob es 802.1X verwenden kann. BICS legt fest, welche Methode verwendet werden kann. Es ist nicht möglich, eine nicht unterstützte Methode zur Authentifizierung eines Geräts festzulegen.

6.2 BICS Funktionalität: Unterstützung von 802.1X

- **Ermöglicht 802.1X-Unterstützung für Switches.**

Im Port Security Manager wird der Switch aktiviert.

- **Legen Sie die Authentifizierungsmethode fest.**

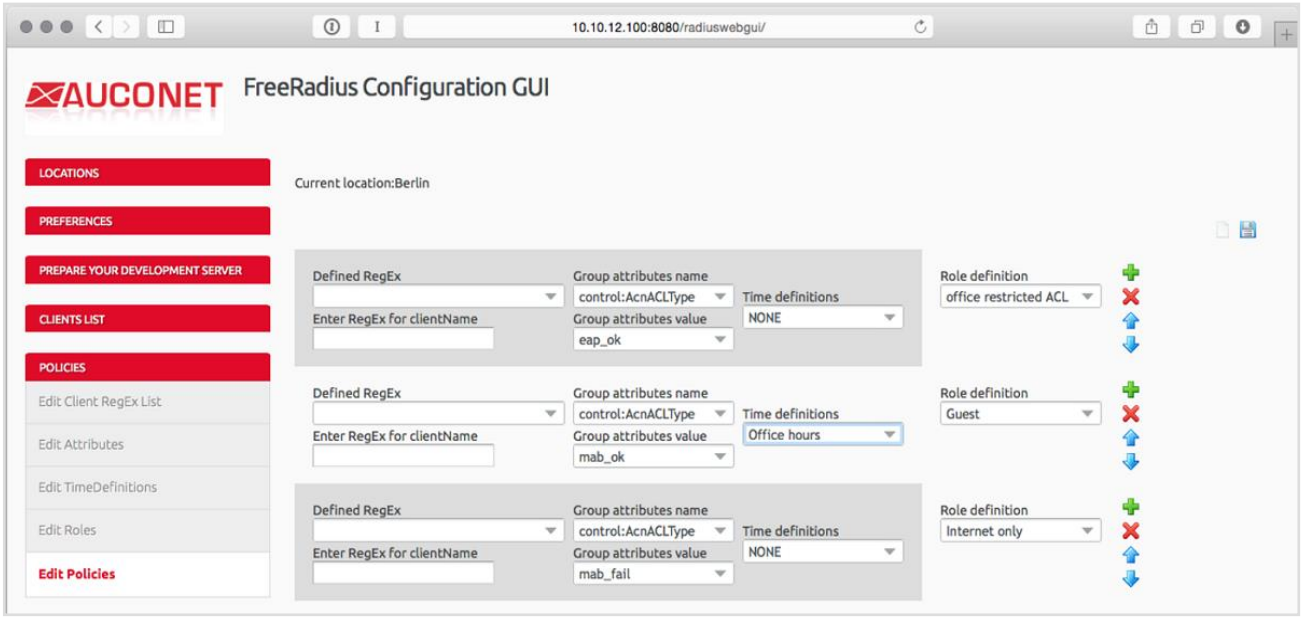
Setzen Sie UserAuth; MACAuth; PWAAuth (Mehrfachauswahl).

- **RADIUS konfigurieren.**

Der Administrator kann den BICS Radius Server über die grafische Benutzeroberfläche konfigurieren.

7. Network-Port Security Management Policy Support

Mit Infraray BICS können Betreiber Verwaltungsrichtlinien festlegen. Mit dem vom RADIUS-Server gewährten Zugriff können Administratoren zusätzliche Rechte setzen.



7 BICS enables simple, menu-driven operation of the Radius server.

7.1 Access control

- **Betreiber können Regeln und Richtlinien festlegen, um unerwünschten Zugriff auf das LAN zu verhindern.**
  Operatoren können detaillierte, flexible Regeln konfigurieren, um den Authentifizierungsprozess einfach einzurichten und zu steuern.

7.2 Funktionalität zur Unterstützung der Netzwerk-Portsicherheit

- **Ressourcen definieren**
  Gruppieren Sie Geräte, Ports und Ressourcen in Ressourcengruppen.

- **Zeitregeln definieren**
  Definieren Sie Zeitdefinitionen auf Stunden-, Tages-, Wochen- und Monatsbasis.

- **Rollen definieren (annehmen, ablehnen, VLAN x zuweisen)**
  Definieren Sie die Authentifizierungsaktionen.

- **Kombinieren Sie alle oben genannten Funktionen in einer Richtliniendefinition.**
  Kombinieren Sie die definierten Richtlinienparameter zu einer Richtlinie, die auf dem verbundenen Endpunkt ausgeführt wird.

8. VLAN Management

Das VLAN-Management erweitert INFRARAY Security um die Möglichkeit, ausgewählte Ports zu konfigurieren und bestimmten VLANs zuzuweisen.

8.1 Feature Beschreibung

- **Stellen Sie Port VLANs für autorisierte Endpunkte ein.**

Weist Endpunkte automatisch einem bestimmten VLAN zu, entsprechend den definierten Richtlinien.

- **Stellen Sie Port VLANs für nicht autorisierte Endpunkte ein.**

Ein unbekannter Endpunkt kann einem "Guest"- oder "Quarantäne"-VLAN zugewiesen und darauf beschränkt werden.

- **VLAN-IDs und VLAN-Namen verwalten.**

Eine zentrale Ansicht und Bedienoberfläche zum Erstellen, Verwalten und ggf. Löschen von VLANs..

8.2 Funktionen, die dieses Feature unterstützen

- **Der Betreiber kann VLANs vordefinieren.**

Definieren Sie beliebig viele VLANs in der Verwaltungsoberfläche.

- **Der Betreiber kann Richtlinien so vorgeben, dass die folgenden Funktionen automatisch und in Echtzeit von BICS ausgeführt werden.**

Setzen der Switch-/Port-VLAN-Einstellungen

Bei einer unbekannten MAC-Adresse setzt BICS den Port-Status auf Unauthorized (Herunterfahren des Ports) oder weist den Port einem Quarantäne-VLAN zu.

Stellen Sie das VLAN auf autorisierte, nicht autorisierte und unbenutzte Ports ein.

- **BICS ermöglicht es dem Betreiber, spezifische VLAN-IDs für bestimmte MAC-Adressen festzulegen und die VLAN-Zuweisungsrichtlinien vorzugeben, die BICS automatisch befolgt und in Echtzeit durchsetzt.**

Der Betreiber kann das VLAN definieren, dem MAC-Adressen und Bereiche von MAC-Adressen beim Einloggen eines Endpunktes in das Netzwerk automatisch zugewiesen werden. Mit anderen Worten, wenn das Gerät, das die Anmeldung versucht, eine bekannte MAC-Adresse hat, kann BICS dieses Gerät sofort einem vordefinierten VLAN zuordnen und gleichzeitig den Port autorisieren, den das neue Gerät verwendet. Wenn sich ein Gerät am Netzwerk anmeldet, sucht BICS die MAC-Adresse in seiner MAC/VLAN-Tabelle, um zu überprüfen, ob diese Adresse einem bestimmten VLAN zugewiesen wurde. Wenn ja, ordnet BICS den verwendeten Port automatisch dem entsprechenden zu.

www.infraray-it.com

Über Infraray

Infraray wurde 1998 von einem deutschen Ingenieurteam mit langjähriger Erfahrung im Bereich IT Operation Management gegründet. Das Unternehmen bietet Lösungen für die Informationstechnologie und bietet Lösungen für Netzwerkmanagement, Netzwerksicherheit, IT-Infrastrukturmanagement, Cloud, Netzwerkautomatisierung und die Steuerung der Geschäftsinfrastruktur.

Infraray BICS ist die Next-Generation-ITOM-Plattform zur Steuerung großer und heterogener Unternehmensnetzwerke. BICS bietet nicht nur Netzwerk-Infrastrukturmanagement für alle Geräte und Endgeräte der Hersteller, sondern dient auch als Grundlage für eine neue Generation von IT-Infrastrukturmanagement.

Infraray ist seit Anfang 2018 Teil der Beta Systems Group.

infraray

Infraray GmbH
Stromstr. 5
10555 Berlin / Germany

Tel. +49 (0) 30 254 690-0
Fax: +49 (0) 30 254 690-199
info@Infraray.com