Zscaler Technical Update
06. März 2024

Round Table: Troubleshooting

Jonas Kugler
Security Engineer
kugler@avantec.ch

Ziel und Ablauf Round Table

- Ziel Round Table
  - Das Ziel des Round Tables ist eine gemeinsame Diskussion zum Wissensaustausch über die Troubleshooting- und Analysemöglichkeiten mit Zscaler sowie über Issues, die gehäuft angetroffen werden.

- Ablauf Round Table
  - Vorstellung Thema #1
  - Diskussionrunde #1
  - Vorstellung Thema #2
  - Diskussionrunde #2
  - Vorstellung Thema #3
  - Diskussionrunde #3

Zscaler Technical Update
06. März 2024

Gefährliches maximal minimieren –
wie wir Sie dabei unterstützen können.

Themen des Round Tables

- Häufige Issues
- Troubleshooting
- Analysemöglichkeiten

Zscaler Technical Update
06. März 2024

AVANTEC
Competence. Security. Trust.

Wir sorgen für höchste IT-Sicherheit –
was uns dabei wichtig ist.

Häufige Issues

AVANTEC
Competence. Security. Trust.

- Captive Portals
- IPv4/IPv6

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Häufige Issues – Captive Portals

- Was zählt für den ZCC als Captive Portal?
  - Webpages mit AUPs
  - Webpages zur Anmeldung am WLAN (Flughäfen, Hotels, etc.)
  - Webpages mit Fehlermeldungen eines Systems im Flow der Kommunikation
  - Redirects und Caution Pages
  - Vieles mehr

Häufige Issues – Captive Portals

- Wie wird ein Captive Portal erkannt? (Primär)
  - ZCPM detectCaptive: Connecting to url: http://gateway.zscaler.net/zcc_conn_test
  - ZCPM detectCaptive: Response Status 403 Length: 35346
  - ZCPM detectCaptive: Captive detected.
  - ZCPM Captive portal detected through URL: http://gateway.zscaler.net/zcc_conn_test

AVANTEC
Competence. Security. Trust.

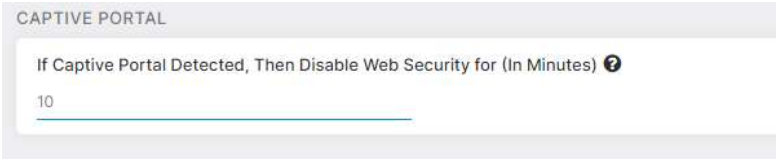
Zscaler Technical Update
06. März 2024

Häufige Issues – Captive Portals

- Wie wird ein Captive Portal erkannt? (Sekundär)
  - Zscaler lädt das Zscaler Default PAC
  - Weicht die erhaltene Antwort vom Default PAC ab, wird ein ein Captive Portal vermutet

Häufige Issues – Captive Portals

- Welche Möglichkeiten bietet der ZCC im Umgang mit Captive Portals?
  - Administration -> Client Connector Support -> App Fail Open



-> Die eingetragene Zeit ist als Maximum zu betrachten, sobald eine Verbindung zum Service Edge möglich ist wird die Web Security enabled

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Häufige Issues – Captive Portals

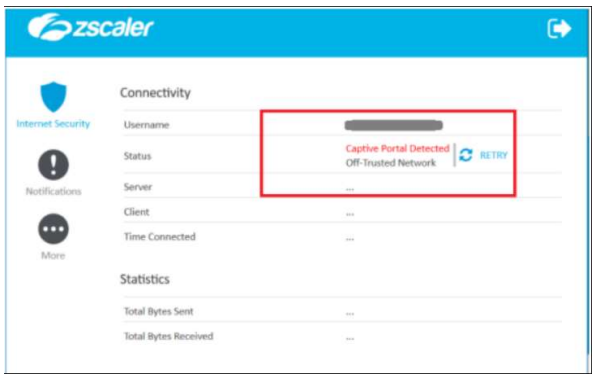
AVANTEC
Competence. Security. Trust.

- Einige Verbindungstests können zu Interferenzen mit der Detection führen und können bei Bedarf bypassed werden (VPN Gateway Bypass)
  - Windows
    - www.msftncsi.com
    - dns.msftncsi.com
    - www.msftconnecttest.com
  - MacOS
    - captive.apple.com
  - Android
    - connectivitycheck.gstatic.com

Häufige Issues – Captive Portals

AVANTEC
Competence. Security. Trust.

- Wie kann dies geprüft werden?
  - Developer Tools im Browser
  - ZCC Service Status
    -> "Captive Portal Detected“
  - Curl

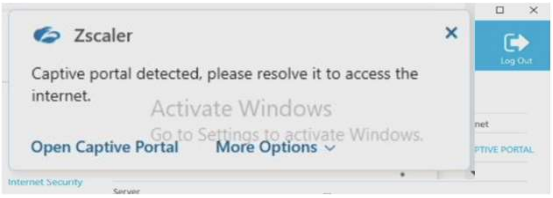


AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Häufige Issues – Captive Portals

- Verbesserungen mit ZCC 4.3+
  - Notifications
  - Captive Portal Handling



Häufige Issues – IPv4/IPv6

- Traffic wird neu plötzlich direkt an IPv6 Destinationen gesendet
  - Traffic nicht durch Zscaler geschützt
  - Traffic von dieser IP möglicherweise auf dem Zeilsystem nicht erlaubt (z.B. bei Azure AD)

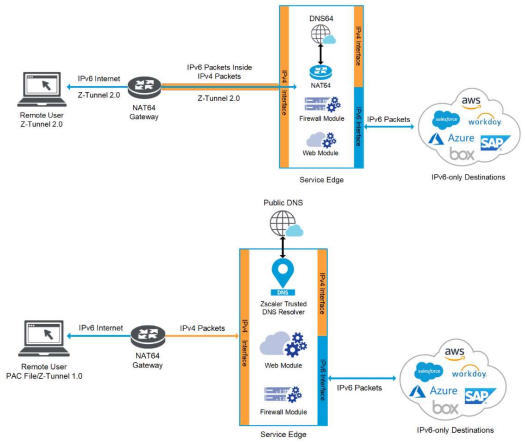
AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Häufige Issues – IPv4/IPv6

AVANTEC
Competence. Security. Trust.

- Wie kann mit IPv6 umgegangen werden?
  - Unterstützung von IPv6 ist gegeben
  - Wachsendes Angebot an IPv6-fähiger Nodes
  - Blockierung von IPv6 im ZCC
  - Priorisierung von IPv4 über IPv6
  - Vollständige Unterstützung von IPv6*



https://help.zscaler.com/zia/understanding-ipv6-support#remote-traffic

Häufige Issues

AVANTEC
Competence. Security. Trust.

Fragen in die Runde:
Haben Sie bereits selbst Probleme mit Captive Portals und/oder IPv6 über Zscaler angetrofen? Wie haben Sie diese gelöst?
Ist der Einsatz von IPv6 in Ihren Umgebungen aktuell ein Thema?

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Damit Gefährliches draussen bleibt –
wer sich dafür auf uns verlässt.

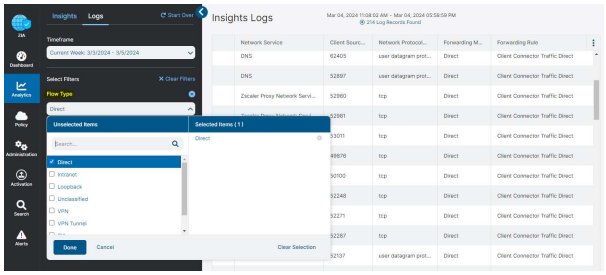
Troubleshooting

- Flow Logging

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Troubleshooting – Flow Logging



- Was bringt Flow Logging?
  - Verbesserte Sichtbarkeit
  - Threat detection und incident response
  - Troubleshooting
- Setzt auf Windows Filtering Platform (WFP) Driver
  -> Nur für Windows Profile nutzbar

Troubleshooting – Flow Logging

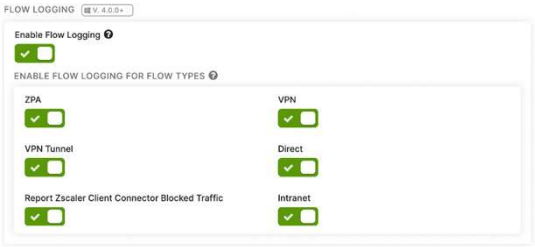
- Flow Types
  - ZPA
  - VPN (outer tunnel)
  - VPN Tunnel (inner tunnel, somit der eigentliche Traffic im Tunnel)
  - ZCC blocked traffic
    - T2 Fallback, IPv6 Drops, Blocks durch Strict Enforcement, Disaster Recovery Blocks
  - Direct
  - Intranet
    - RFC1918, IPv6 Intranet

Zscaler Technical Update
06. März 2024

Troubleshooting – Flow Logging

AVANTEC
Competence. Security. Trust.

- Konfiguration
  - Feature via Support Ticket aktivieren
  - Settings pro App Profil
- Logs
  - Web Insights und Firewall Insights
  - Filtern nach Flow Types möglich



Troubleshooting – Flow Logging

AVANTEC
Competence. Security. Trust.

Fragen in die Runde:
Haben Sie bereits Flow Logging in Ihren Umgebungen im Einsatz? Welche Use Cases konnten Sie damit abdecken bzw. für das Abdecken welcher Use Cases wäre das Feature für Sie interessant?

AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Gefährliches maximal minimieren –
wie wir Sie dabei unterstützen können.

Analysemöglichkeiten

- Reports
  - Security Policy Audit Report
  - Configuration Risk Report
  - System Audit Report
  - SaaS Security Report

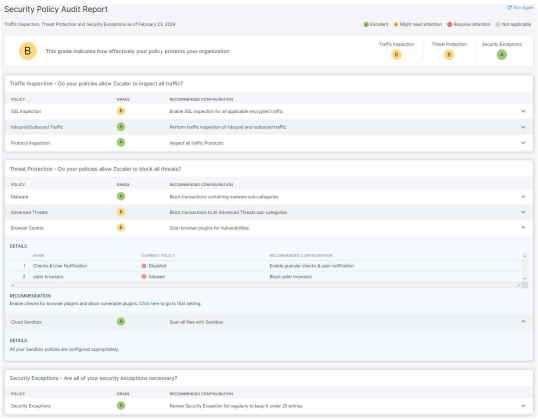
AVANTEC
Competence. Security. Trust.

Zscaler Technical Update
06. März 2024

Analysemöglichkeiten – Security Policy Audit Report

- Bewertung der Security Policy

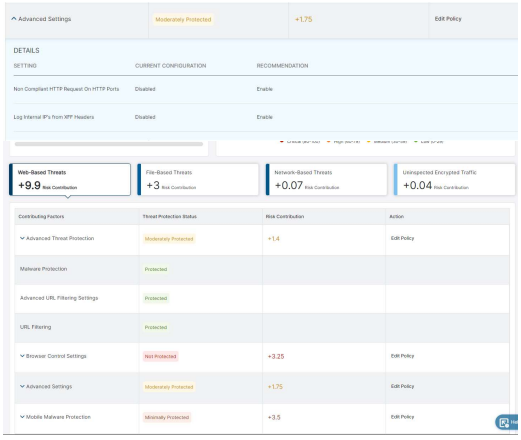
- Kategorien
  - Traffic Inspection
  - Threat Protection
  - Security Exceptions



Analysemöglichkeiten - Configuration Risk Report

- Konsolidierter Risk Score

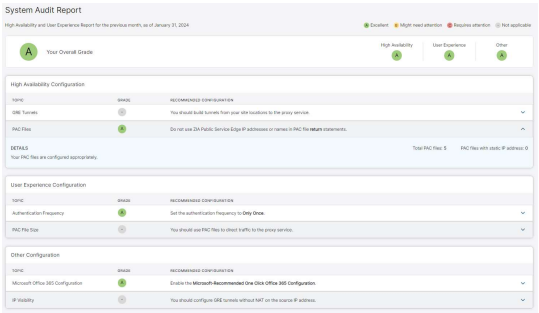
- Kategorien
  - Web-Based Threats
  - File-Based Threats
  - Network-Based Threats
  - Uninspected Encrypted Traffic



Zscaler Technical Update
06. März 2024

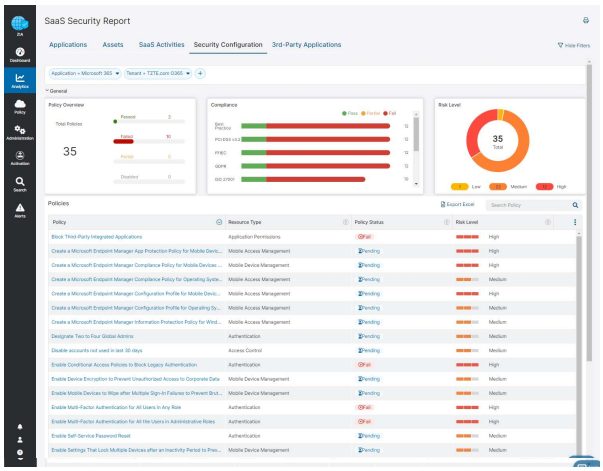
Analysemöglichkeiten - System Audit Report

- Bewertung der System-Konfiguration
- Kategorien
  - High Availability Configuration
  - User Experience Configuration
  - Other Configuration



Analysemöglichkeiten – Saas Security Report

- Übersicht zu Saas Traffic/Applikationen
- Kategorien
  - Applications
  - Assests
  - SaaS Activities
  - Security Configuration
    - Konfiguration nötig
      Policy > SaaS Security Posture Management
  - 3rd Party Aplications



Zscaler Technical Update
06. März 2024

Analysemöglichkeiten

Fragen in die Runde:
Welche Reports haben Sie bereits gekannt und zur Analyse Ihrer bestehenden Konfiguration genutzt?
Nutzen Sie neben den vorgstellten Reports noch andere Reports oder Tools von Zscaler um das bestehende Setup zu Analysieren und Überarbeiten?

Offene Disskussionsrunde

Fragen in die Runde:
Haben Sie Themen im Zusammenhang mit Zscaler Troubleshooting, welche Sie gerne hier im Plenum besprechen würden um auf den grossen Erfahrungsschatz aller anwesenden Teilnehmer zurückgreifen zu können?

AVANTEC
Competence. Security. Trust.