Begonnen am	Mittwoch, 22. November 2023, 10:01
Status	Beendet
Beendet am	Mittwoch, 22. November 2023, 10:32
Verbrauchte Zeit	30 Minuten 26 Sekunden
Bewertung	**35,8** von 42,0 (**85**%)

Frage **1**

Richtig

Erreichte Punkte 2,0 von 2,0

Eine VPN Lösung (egal ob HW- / SW-basiert) erfüllt immer mindestens die folgenden wichtige Aufgaben.
Wählen Sie die korrekten 3 Antworten aus.

- [x] 1. Verwaltung der Schlüssel zur Datenverschlüsselung und Authentifikation ✔ Korrekt (1/3) Punktzahl erhalten
- [ ] 2. Jede VPN-Lösung muss auf einem gehärteten System laufen um die Sicherheit zu garantieren.
- [ ] 3. Scanning des gesamten VPN-Verkehrs nach Malware
- [x] 4. Authentisierung der Teilnehmer einer VPN-Verbindung und der ausgetauschten Datenpakete ✔ Korrekt (1/3) Punktzahl erhalten
- [x] 5. Verschlüsselung des Datenverkehrs der 2 Partner ✔ Korrekt (1/3) Punktzahl erhalten

Die Antwort ist richtig.

Die richtigen Antworten sind:
Verschlüsselung des Datenverkehrs der 2 Partner,

Authentisierung der Teilnehmer einer VPN-Verbindung und der ausgetauschten Datenpakete,

Verwaltung der Schlüssel zur Datenverschlüsselung und Authentifikation

Frage **2**

Richtig

Erreichte Punkte 3,0 von 3,0

Thema SSL-VPN

Entscheiden Sie für jeden Punkt, ob dies ein Vor- oder Nachteil ist:

- Geschwindigkeit beim SSL-VPN Verbindungsaufbau = Nachteil ✖
- Aufwand für clientseitige Softwareinstallation SSL-VPN = Vorteil ✖
- Aufwand für clientseitige Administration (SSL-VPN) = Vorteil ✔
- HW-Anforderungen bei Java-Applets / Active-X Komponenten für SSL-VPN = Nachteil ✔
- Aufwand für Firewall-Regeln = Vorteil ✖

Die Antwort ist richtig.

auf Seite 125 im M-145 PDF sehen Sie die Vor-/Nachteile in der Liste 7.3.3 im Text.

Die richtige Antwort lautet:

Thema SSL-VPN

Entscheiden Sie für jeden Punkt, ob dies ein Vor- oder Nachteil ist:

- Geschwindigkeit beim SSL-VPN Verbindungsaufbau = [Nachteil]
- Aufwand für clientseitige Softwareinstallation SSL-VPN = [Vorteil]
- Aufwand für clientseitige Administration (SSL-VPN) = [Vorteil]
- HW-Anforderungen bei Java-Applets / Active-X Komponenten für SSL-VPN = [Nachteil]
- Aufwand für Firewall-Regeln = [Vorteil]

Kommentar:
korrigiert

Frage **3**

Falsch

Erreichte Punkte 0,0 von 1,0

Ordnen Sie korrekt zu:

AH ✖ verschlüsselt das ganze Paket

ESP ✖ verschlüsselt nur den Header

Die Antwort ist falsch

Seite 119/120 im Buch

Die richtige Antwort lautet:
Ordnen Sie korrekt zu:

[ESP] verschlüsselt das ganze Paket

[AH] verschlüsselt nur den Header

Frage **4**

Falsch

Erreichte Punkte 0,0 von 1,0

Die MITM-Attacke läuft auf Layer-3 und ist nur möglich wenn sich der Angreifer zwischen den Empfänger und den Sender einklinken kann.

Bitte wählen Sie eine Antwort:

◉ Wahr ✖

○ Falsch

MITM Attacken sind Layer-2 Attacken. Theorie PDF auf Seite 91 lesen.

Theorie PDF auf Seite 91 lesen.

Die richtige Antwort ist 'Falsch'.

Frage **5**

Richtig

Erreichte Punkte 1,0 von 1,0

Ist es korrekt, dass bei einem VPN für den Austausch der Schlüssel zwischen zwei Kommunikationspartnern meistens das Diffie-Hellmann-Protokoll eingesetzt wird?

Bitte wählen Sie eine Antwort:

- Wahr ✔
- Falsch

Korrekt, das Diffie-Hellman-Protokoll ist dazu geeignet.

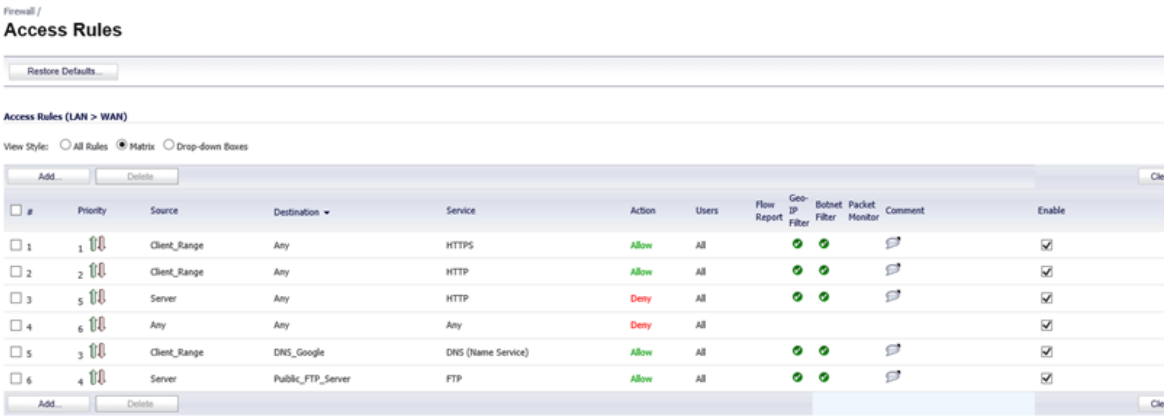
PDF Seite 126 mittlerer Abschnitt nachlesen.

Die richtige Antwort ist 'Wahr'.

Frage **6**

Teilweise richtig

Erreichte Punkte 0,7 von 1,0



Wählen Sie **alle korrekten Aussagen** zum Firewall-Ruleset und der Verarbeitung, passend zum gezeigten Ruleset der SonicWall Firewall im Bild hier.
Vergrössern Sie das Bild um alles korrekt sehen und interpretieren zu können.

Wählen Sie eine oder mehrere Antworten:

- [x] a. Die Regeln erlauben dem Server **jeden** FTP Dienst zu erreichen ✖ Nein, es ist zwar der FTP Server zugelassen aber nur das Adressobjekt im Public-FTP-Server.
- [x] b. Das Ruleset an sich ist korrekt, die Reihenfolge jedoch von der Anzeige-Sortierung her falsch sortiert (ist gefährlich in der Praxis). ✔ ja, genau dieser Fehler wurde uns zum "Verhängnis" weil daraufhin eine falsche Rule eingefügt worden war.
- [ ] c. Gemäss diesem Ruleset darf der Server eigentlich keine DNS Abfragen im Internet machen.
- [x] d. In dieser Firewall ist die Any / Any / Any / Deny - Regel die letzte Regel in der Verarbeitung und das stimmt so. ✔
- [ ] e. Die Regeln erlauben dem Server das Internet mit dem HTTP Protokoll zu nutzen

Die Antwort ist teilweise richtig.

Sie haben 2 richtig ausgewählt.
Die richtigen Antworten sind: Das Ruleset an sich ist korrekt, die Reihenfolge jedoch von der Anzeige-Sortierung her falsch sortiert (ist gefährlich in der Praxis)., Gemäss diesem Ruleset darf der Server eigentlich keine DNS Abfragen im Internet machen. ,
In dieser Firewall ist die Any / Any / Any / Deny - Regel die letzte Regel in der Verarbeitung und das stimmt so.

Frage **7**

Richtig

Erreichte Punkte 2,0 von 2,0

Ordnen Sie die bekannten Dienste/Anwendungen den korrekten Portnummern zu:

HTTP = 80 ✔

SSL = 443 ✔

SFTP = 22 ✔

POP3 = 110 ✔

DNS = 53 ✔

SNMP Trap = 162 ✔

SMTP = 25 ✔

Real-Time Streaming Protocol (RTSP) = 554 ✔

Citrix ICA-Protokoll = 1494 ✔

Microsoft SQL-Server = 1433 ✔

Server Message Block (SMB) over TCP/IP = 445 ✔

Die Antwort ist richtig

Siehe https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-ports.html

Die richtige Antwort lautet:
Ordnen Sie die bekannten Dienste/Anwendungen den korrekten Portnummern zu:

HTTP = [80]
SSL = [443]
SFTP = [22]
POP3 = [110]
DNS = [53]
SNMP Trap = [162]
SMTP = [25]
Real-Time Streaming Protocol (RTSP) = [554]
Citrix ICA-Protokoll = [1494]
Microsoft SQL-Server = [1433]
Server Message Block (SMB) over TCP/IP = [445]

Frage **8**

Richtig

Erreichte Punkte 1,0 von 1,0

Stimmt es, dass ESP die IP-Protokollnummer Nr. 51 verwendet?

Bitte wählen Sie eine Antwort:

- Wahr
- Falsch ✔

Korrekt, es ist die IP-Protokollnummer 50 und nicht 51
Lesen Sie dies auf der Seite 120 im Bereich 7.2.2 nach.

Die richtige Antwort ist 'Falsch'.

Frage **9**

Richtig

Erreichte Punkte 1,0 von 1,0

Firewall-Queues (Rulesets) werden von **unten nach oben** bearbeitet und der Prozess endet, wenn die 1. Regel zutrifft.

Bitte wählen Sie eine Antwort:

- Wahr
- Falsch ✔

Die richtige Antwort ist 'Falsch'.

Frage **10**

Richtig

Erreichte Punkte 2,0 von 2,0

Füllen Sie den Lückentext mit "Drag&Drop" so aus, dass die entstehenden Aussagen korrekt sind:

VPN's verwenden ESP, um die [Vertraulichkeit] ✔ der übertragenen Daten sicherzustellen. Bei einer Vernetzung von zwei Standorten (Site-to-Site) kommt ESP im [Tunnel] ✔ -Modus zur Anwendung. Bei VPN-Verbindungen zwischen 2 Rechnern kommt ESP grundsätzlich im [Transport] ✔ -Modus zur Verfügung. ESP basiert auf [IP] ✔ . Die Abkürzung "ESP" im VPN-Bereich bedeutet ausformuliert: [Encapsulated] ✔ [Security] ✔ [Payload] ✔ .

Die Antwort ist richtig.

Im PDF finden Sie diese Informationen auf der Seite 120 Bereich 7.2.2

Die richtige Antwort lautet:
Füllen Sie den Lückentext mit "Drag&Drop" so aus, dass die entstehenden Aussagen korrekt sind:

VPN's verwenden ESP, um die [Vertraulichkeit] der übertragenen Daten sicherzustellen. Bei einer Vernetzung von zwei Standorten (Site-to-Site) kommt ESP im [Tunnel]-Modus zur Anwendung. Bei VPN-Verbindungen zwischen 2 Rechnern kommt ESP grundsätzlich im [Transport]-Modus zur Verfügung. ESP basiert auf [IP]. Die Abkürzung "ESP" im VPN-Bereich bedeutet ausformuliert: [Encapsulated] [Security] [Payload].

Frage **11**

Teilweise richtig

Erreichte Punkte 0,5 von 1,0

Sie setzen ein IPS-System bei Ihnen ein. Welche Zielobjekte werden in der Arbeit des Intrusion Prevention Systems analysiert? Wählen Sie hier alle korrekten Aussagen aus.

- [x] a. nach bestimmten Mustern/Patterns, anhand deren ein Angriff erkannt werden kann ✔ Korrekt. Ist ein Teilbereich.
- [ ] b. Nach "protokollfremden" eingebetteten Programmcodes bzw. ausführbaren Befehlen innerhalb der Applikationsdaten eines Datenpaketes
- [ ] c. nach den Einträgen im Audit-Logs des Netzwerkservers
- [ ] d. nach unerlaubten Netzaktivitäten wie z.B. "Peer-to-Peer"-Funktionen (P2P) oder verbotenen Nachrichtendiensten (z.B. Instant Messaging wie Skype / Twitter)
- [x] e. nach dem Abruf von verbotenen Dateninhalten aus dem Internet wie Pornografie, Gewaltszenen etc. ✔ Korrekt. Ist ein Teilbereich.

Die Antwort ist teilweise richtig.

Sie haben 2 richtig ausgewählt.
Seite 93 im PDF beachten mit den korrekten Aussagen im PDF auf Seite 133.

Die richtigen Antworten sind:
nach bestimmten Mustern/Patterns, anhand deren ein Angriff erkannt werden kann,

Nach "protokollfremden" eingebetteten Programmcodes bzw. ausführbaren Befehlen innerhalb der Applikationsdaten eines Datenpaketes,

nach unerlaubten Netzaktivitäten wie z.B. "Peer-to-Peer"-Funktionen (P2P) oder verbotenen Nachrichtendiensten (z.B. Instant Messaging wie Skype / Twitter),

nach dem Abruf von verbotenen Dateninhalten aus dem Internet wie Pornografie, Gewaltszenen etc.

Frage **12**

Richtig

Erreichte Punkte 3,0 von 3,0

Ordnen Sie die VPN Protokollnamen den Protokollen korrekt zu, damit jeweils korrekte Aussagen entstehen:

[[1]] = Dieses Übertragungsprotokoll dient zur Sicherstellung der Integrität und der Authentizität eines Datenpakets.

[[2]] = Dieses Übertragungsprotokoll dient zur Verschlüsselung der zu übertragenden Daten

[[3]] = Dieses Protokoll eignet sich auch für zeitkritische Anwendungen im Gegensatz zum [[4]] Protokoll.

Wählen Sie für den Punkt [1]:	Authentication Header (AH)	✔
Wählen Sie für den Punkt [2]:	Encapsulated Security Payload (ESP)	✔
Wählen Sie für den Punkt [3]:	UDP	✔
Wählen Sie für den Punkt [4]:	TCP	✔

Die Antwort ist richtig.

Die richtige Antwort ist:
Wählen Sie für den Punkt [1]: → Authentication Header (AH),

Wählen Sie für den Punkt [2]: → Encapsulated Security Payload (ESP),

Wählen Sie für den Punkt [3]: → UDP,

Wählen Sie für den Punkt [4]: → TCP

Frage **13**

Richtig

Erreichte Punkte 2,0 von 2,0

Ordnen Sie die Aussagen korrekt zu.

End-to-End-VPN	Hier werden 2 Rechnersysteme miteinander verbunden	✔
Site-to-Site-VPN	Hier werden Netzwerke miteinander verbunden	✔
End-to-Site-VPN	Hier werden Fernzugriffe (Remote Access) auf Netzwerke möglich	✔

Die Antwort ist richtig.

Die richtige Antwort ist:
End-to-End-VPN → Hier werden 2 Rechnersysteme miteinander verbunden,

Site-to-Site-VPN → Hier werden Netzwerke miteinander verbunden,

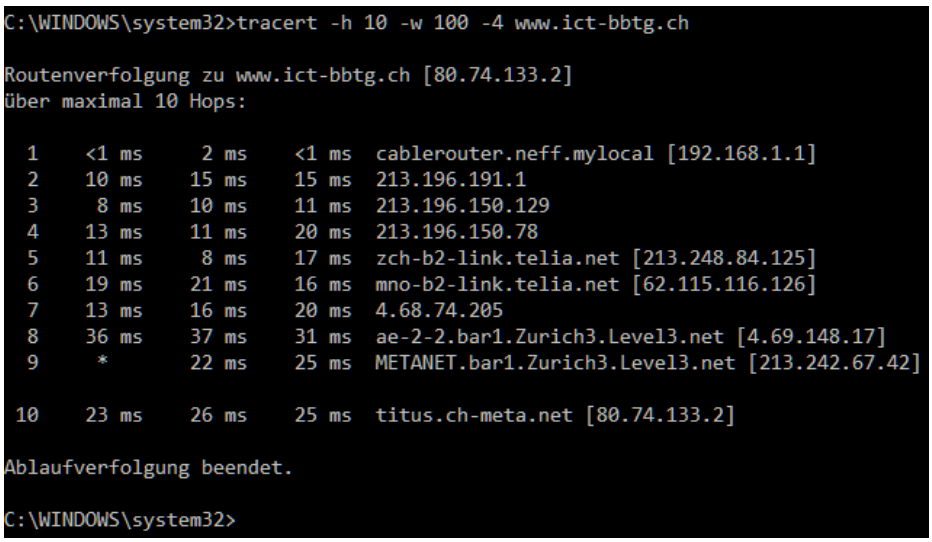
End-to-Site-VPN → Hier werden Fernzugriffe (Remote Access) auf Netzwerke möglich

Frage **14**

Richtig

Erreichte Punkte 1,0 von 1,0

Traceroute mit Optionen:
Ordnen Sie die für das Bild korrekte Aussage zu:



-h 10 -w 100 -4 bedeutet:

mache einen traceroute mit ipv4 zur Adresse www.ict-bbtg.ch, über maximal 10 hops mit einem Zeitlimit von 100ms.	diese Antwort ist korrekt. ✔
mache einen traceroute mit ipv6 zur Adresse www.ict-bbtg.ch, über maximal 10 hops mit einem Zeitlimit von 100ms.	diese Antwort ist falsch. ✔
mache einen traceroute mit ipv4 zur Adresse www.ict-bbtg.ch, über maximal 100 hops mit einem Zeitlimit von 10ms.	diese Antwort ist falsch. ✔

Die Antwort ist richtig

Die richtige Antwort ist: mache einen traceroute mit ipv4 zur Adresse www.ict-bbtg.ch, über maximal 10 hops mit einem Zeitlimit von 100ms. → diese Antwort ist korrekt., mache einen traceroute mit ipv6 zur Adresse www.ict-bbtg.ch, über maximal 10 hops mit einem Zeitlimit von 100ms. → diese Antwort ist falsch., mache einen traceroute mit ipv4 zur Adresse www.ict-bbtg.ch, über maximal 100 hops mit einem Zeitlimit von 10ms. → diese Antwort ist falsch.

Frage **15**

Teilweise richtig

Erreichte Punkte 0,8 von 1,0

Wählen Sie alle Geräte/Dienste im Netzwerk, welche sicherheitsrelevante Dienste/ Services anbieten können.

Wählen Sie eine oder mehrere Antworten:

- [ ] a. WLAN Router
- [x] b. VPN-Server ✔ Korrekt, ist ein Teilpunkt.
- [ ] c. HUB
- [x] d. Proxy-Dienst / Server ✔ Korrekt, ist ein Teilpunkt.
- [x] e. Firewall ✔ Korrekt, ist ein Teilpunkt.

Die Antwort ist teilweise richtig.

Sie haben 3 richtig ausgewählt.
Die richtigen Antworten sind: Firewall, Proxy-Dienst / Server, WLAN Router, VPN-Server

Frage **16**

Richtig

Erreichte Punkte 2,0 von 2,0

Wählen Sie die 3 korrekten Antwortmöglichkeiten aus unserem Theorie-PDF-File, welche das Arbeitsprinzip einer Firewall beschreiben.

Wählen Sie eine oder mehrere Antworten:

- [ ] a. Backward-Queue
- [x] b. Input-Queue ✔ Korrekt! Ist ein Teilpunkt.
- [x] c. Output-Queue ✔ Korrekt! Ist ein Teilpunkt.
- [x] d. Forward-Queue ✔ korrekt! Ist ein Teilpunkt.
- [ ] e. Management-Queue
- [ ] f. Middle-Tier-Queue

Die Antwort ist richtig

Seite 83 PDF zeigt das Arbeitsprinzip einer Firewall mit allen Queues und Verarbeitungsschritten.

Die richtigen Antworten sind: Forward-Queue, Input-Queue, Output-Queue

Frage **17**

Richtig

Erreichte Punkte 1,0 von 1,0

Muss ein Switchport, welcher mehreren VLANs zugewiesen wurde, immer "tagged" sein?

Bitte wählen Sie eine Antwort:

- (●) Wahr ✔
- ( ) Falsch

Korrekt!

PDF Seite 70 Mitte Bereich "Tagged" lesen.

Ein "tagged" Port gehört i.d.R. mehreren VLANs an. Wenn ein Switchport mehreren VLANs zugewiesen wird, muss der entsprechende Port zwingend "tagged" sein.

Die richtige Antwort ist 'Wahr'.

Frage **18**

Teilweise richtig

Erreichte Punkte 0,6 von 1,0

Füllen Sie den Lückentext aus, dass die Aussage korrekt ist:

Die Positionierung einer Firewall in einem Netzwerk ist sehr wichtig. Bei einem zweistufigen Firewallkonzept trennt **von innen nach aussen gesehen**, die "erste" Firewall die Zonen WAN ✖ und DMZ ✔ . Die "zweite" Firewall trennt die Zonen DMZ ✔ und LAN ✖ ab. Direkte Zugriffe aus Zone WAN ✔ in Zone LAN ✔ sind zu vermeiden. Von extern erreichbare Dienste werden deshalb in die Zone DMZ ✔ installiert und können mit NAT / Filtering ✖ und PAT ✖ geschützt werden.

Die Antwort ist teilweise richtig.

Sie haben 5 richtig ausgewählt.
Die richtige Antwort lautet:
Füllen Sie den Lückentext aus, dass die Aussage korrekt ist:

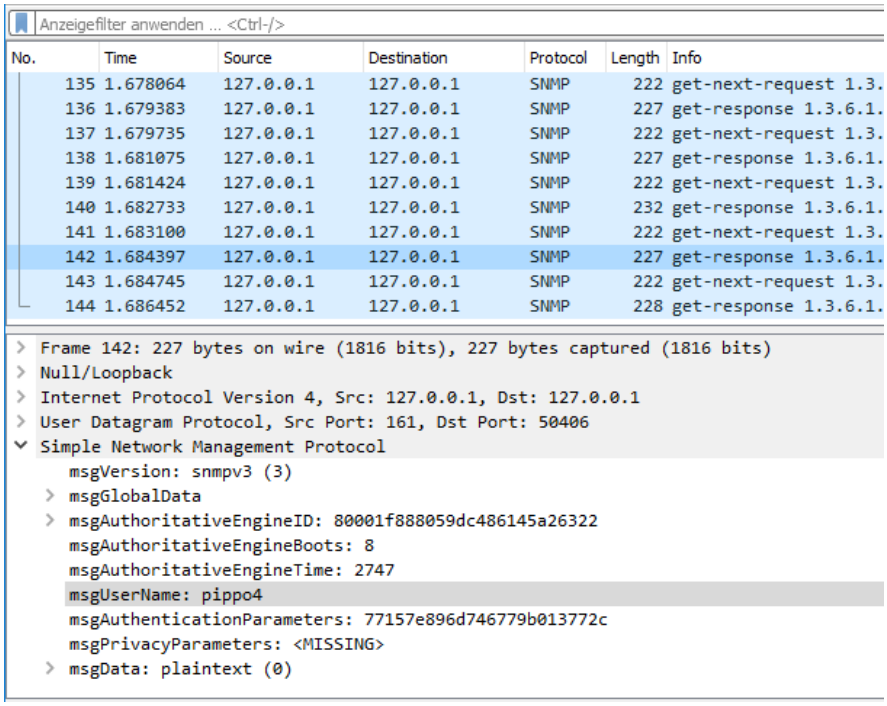
Die Positionierung einer Firewall in einem Netzwerk ist sehr wichtig. Bei einem zweistufigen Firewallkonzept trennt **von innen nach aussen gesehen**, die "erste" Firewall die Zonen [LAN] und [DMZ]. Die "zweite" Firewall trennt die Zonen [DMZ] und [WAN] ab. Direkte Zugriffe aus Zone [WAN] in Zone [LAN] sind zu vermeiden. Von extern erreichbare Dienste werden deshalb in die Zone [DMZ] installiert und können mit [PAT] und [NAT / Filtering] geschützt werden.

Frage **19**

Richtig

Erreichte Punkte 1,0 von 1,0

Welches Protokoll (mit der Versionsnummer) wird hier verwendet?



Antwort: SNMPv3 ✔

korrekt!

Die richtige Antwort ist: snmp v3

Frage **20**

Richtig

Erreichte Punkte 1,0 von 1,0

VPN bedeutet, dass Daten über das Internet in einem "Tunnel" normalerweise verschlüsselt vom Sender zum Empfänger und/oder umgekehrt übertragen werden können.

Bitte wählen Sie eine Antwort:

- (●) Wahr ✔
- ( ) Falsch

korrekt

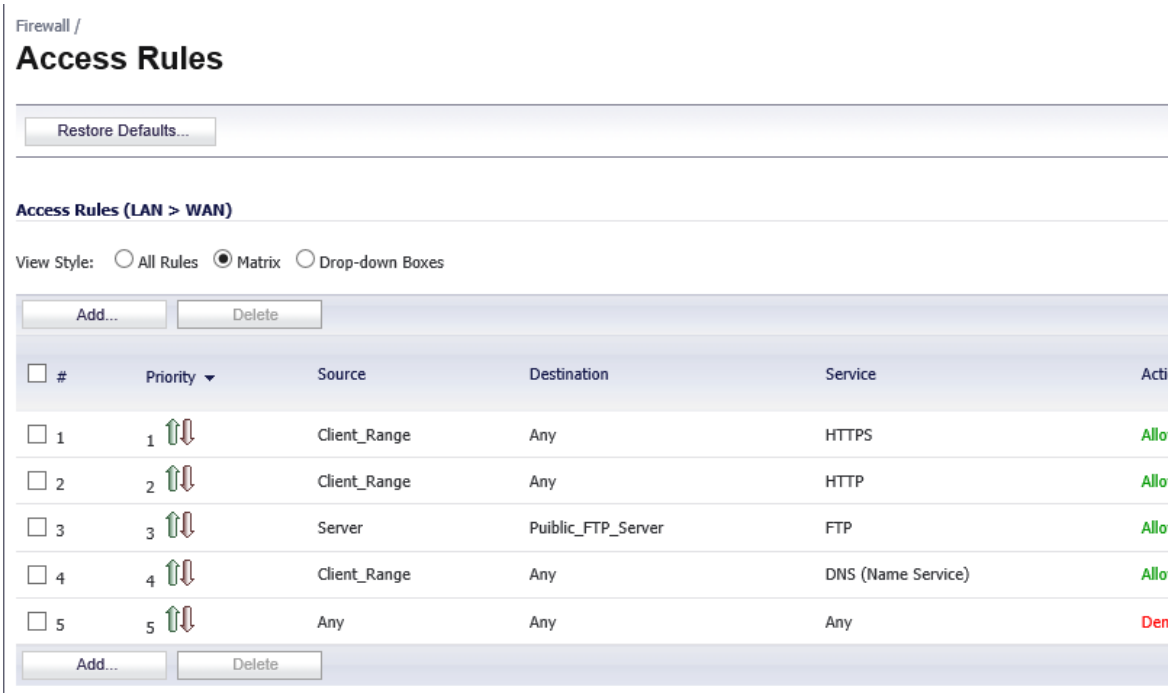
Die richtige Antwort ist 'Wahr'.

Frage **21**

Falsch

Erreichte Punkte 0,0 von 1,0

Finden Sie diese Schwachstelle im Ruleset dieser Firewall?



Wählen Sie eine Antwort:

- a. die Schwachstelle ist der FTP-Server (Regel 3) ✖ Nein, das ist nicht korrekt. Regel #4 ist das Problem. Niemals "global" die DNS Anfragen zulassen. Spezifizieren Sie jeweils Ihren DNS bzw. den Ihres Providors.
- b. die Schwachstelle ist der DNS-Server (Regel 4)
- c. die Schwachstelle sind die Clients (Regel 1+2)
- d. es gibt keine Schwachstelle, alles ist korrekt

Die Antwort ist falsch

Die richtige Antwort ist: die Schwachstelle ist der DNS-Server (Regel 4)

Frage **22**

Richtig

Erreichte Punkte 1,0 von 1,0

Wie heisst der Befehl, welcher es auf einem **entfernten** Webserver (im Internet) herauszufinden, welche Dienste/Ports verfügbar sind?
Das gesuchte Werkzeug ist bei Linux standardmässig installiert, bei Windows jedoch nur als Zusatztool und muss separat installiert werden?
Der Befehl selber heisst bei beiden OS gleich... Finden Sie den korrekten Befehl.

Antwort: nmap ✔

Korrekt. Dieser Befehl ist im Linux-OS standardmässig installiert, muss aber bei Windows separat installiert werden.

Erklärung/Korrekte Lösung:

Nmap is a Network mapping tool. That means it's used to discover informations about hosts on a network (their ip, open ports, etc). Whereas Netstat is a network statistic tool used to list active connections from and to your computer. See https://en.wikipedia.org/wiki/Netstat.

Quelle2: http://www.differencebetween.net/technology/difference-between-nmap-and-netstat/
Zusammengefasst: netstat zeigt die Statistik Informationen des Geräts an, währenddessen mnap aktiv die Geräte im Netzwerk pingt und auf offene Ports abscannt.

Differenzerklärungen:
https://nextdoorsec.com/de/netstat-vs-nmap-vs-netcat-verstehen-der-unterschiede/

Die richtige Antwort ist: nmap

Frage **23**

Richtig

Erreichte Punkte 1,0 von 1,0

Das Aushandeln der Sicherheitsmodalitäten zwischen zwei Kommunikationspartnern (Methoden Authentisierung und Verschlüsselung) wird vom IKE-Protokoll übernommen.

Ist dies korrekt?

Bitte wählen Sie eine Antwort:

- (●) Wahr ✔
- ( ) Falsch

korrekt

Die richtige Antwort ist 'Wahr'.

Frage **24**

Teilweise richtig

Erreichte Punkte 1,3 von 2,0

Wählen Sie **3 besten** (von 5 möglichen) Massnahmen aus, welche es Ihnen erlauben, das ausgefallene Netzwerk schnell wieder online zu bringen:

Wählen Sie eine oder mehrere Antworten:

- [x] a. Aktuelle Konfigurationseinstellungen des ausgefallenen Netzwerkgerätes sind vorhanden. ✔ Korrekt, ist einer der Teilpunkte!
- [ ] b. Alte Konfigurationsanpassungen sind nicht bekannt.
- [ ] c. Wir haben einen Wartungsvertrag für das Gerät oder ein Ersatzgerät im Hause
- [x] d. Die technische Dokumentation und Techniker-Anleitung ist auf dem neuesten Stand und zugreifbar. ✔ Korrekt, ist einer der Teilpunkte!
- [x] e. Alte Firmware ist auf dem Netzwerk noch vorhanden / verfügbar ✖ nicht ganz korrekt. Es gibt 3 bessere Punkte dafür in der Auswahl! Sie sollten immer jeweils in Sicherheitgeräten die neueste released Firmware einsetzen.

Die Antwort ist teilweise richtig.

Sie haben 2 richtig ausgewählt.
Die richtigen Antworten sind: Aktuelle Konfigurationseinstellungen des ausgefallenen Netzwerkgerätes sind vorhanden., Wir haben einen Wartungsvertrag für das Gerät oder ein Ersatzgerät im Hause, Die technische Dokumentation und Techniker-Anleitung ist auf dem neuesten Stand und zugreifbar.

Frage **25**

Richtig

Erreichte Punkte 1,0 von 1,0

Ist es korrekt, dass die Segmentierung von VLANs auf Layer 3 des OSI-Modells arbeitet?

Bitte wählen Sie eine Antwort:

- ○ Wahr
- ◉ Falsch ✔

korrekt. Die Segmentierung (VLAN Einteilung) findet auf Layer 2 des OSI-Modells statt.

Die Segmentierung von VLANs arbeitet auf Layer-2. Erst der Einsatz von Routing-Funktionalitäten (oder Layer-3 Switches), ermöglichen die Weiterleitung auf andere Netzwerksegmente. Layer 2 blockiert die Broadcasts.

https://blog.michael-wessel.de/2014/10/31/vlans-netzwerksegmentierung-leicht-gemacht/

Die richtige Antwort ist 'Falsch'.

Frage **26**

Richtig

Erreichte Punkte 2,0 von 2,0

Welche unterschiedlichen Firewall-Arten sind verfügbar. Wählen Sie die richtigen 3 aus den 6 angebotenen Möglichkeiten aus.

Wählen Sie eine oder mehrere Antworten:

- [ ] a. Paketfilter + Contentfiltering + VLAN Firewall
- [x] b. Paketfilter + Stateful Inspection (SPI) + Application Layer Firewall (ALF) ✔
- [ ] c. Fast-Ethernet-SPI-Content-Firewall
- [x] d. Paketfilter ✔
- [ ] e. Ethernet-Stateful-Connection Checking
- [x] f. Paketfilter + Stateful Inspection (SPI) ✔

Die Antwort ist richtig

Die richtigen Antworten sind: Paketfilter, Paketfilter + Stateful Inspection (SPI), Paketfilter + Stateful Inspection (SPI) + Application Layer Firewall (ALF)

Frage **27**

Falsch

Erreichte Punkte 0,0 von 1,0

Firewall Regeldefinitionen sind standardisiert und über viele Hersteller gleich.

Bitte wählen Sie eine Antwort:

- (•) Wahr ✖
- ( ) Falsch

Leider ist das nicht so. Je nach Hersteller, Typ und Modell können die Befehle und Kommandos für Firewall-Geräte sehr unterschiedlich sein. Dazu muss vom Hersteller des Geräts jeweils das Manual zu Rate gezogen werden. Beispiele dazu finden Sie im Theorie PDF Seite 84 in der Regel-Tabelle.

Die richtige Antwort ist 'Falsch'.

Frage **28**

Richtig

Erreichte Punkte 1,0 von 1,0

Richtig oder falsch?

ARP ist ein Layer-2 Protokoll, welches eine Layer 3 IP nutzt, um eine Layer 2 MAC Adresse zu ermitteln.

Bitte wählen Sie eine Antwort:

- Wahr ✔
- Falsch

korrekt!

Quelle Seite 40 oder hier: https://networkencyclopedia.com/arp-command/

Die richtige Antwort ist 'Wahr'.

Frage **29**

Richtig

Erreichte Punkte 1,0 von 1,0

Ist es korrekt, dass ein RADIUS Service den Supplicanten prüft und den Authenticator anweist, den jeweiligen Netzwerkzugang zu gewähren oder zu verhindern?

Bitte wählen Sie eine Antwort:

- Wahr ✔
- Falsch

Korrekt!

Die richtige Antwort ist 'Wahr'.

Frage **30**

Richtig

Erreichte Punkte 1,0 von 1,0

Geben Sie den für APIPA reservierten gesamten Adressbereich in folgendem Format an:

xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

Antwort: 169.254.0.0-169.254.255.255 ✔

korrekt, siehe PDF-Buch Lösungen Seite 132. Weitere Quelle:
https://www.geeksforgeeks.org/what-is-apipa-automatic-private-ip-addressing/

https://www.geeksforgeeks.org/what-is-apipa-automatic-private-ip-addressing/
der Netzwerkbereich hier lautet wie in der Lösung erwähnt: **169.254.0.0/16 (169.254.0.0 – 169.254.255.255)**
Der effektiv verfügbare IP-Bereich ist:
169.254.0.1 to 169.254.255.254 also 65534 IP-Adressen

Die richtige Antwort ist: 169.254.0.0-169.254.255.255

Frage **31**

Richtig

Erreichte Punkte 1,0 von 1,0

Wählen Sie alle Optionen korrekt aus, welche zu dieser Aussage passen.

Im Unterschied zum IP-Protokoll beinhaltet das sichere Internetprotokoll (IPSec):

Wählen Sie eine oder mehrere Antworten:

- [ ] a. schnelle Übertragung
- [ ] b. starke Passwörter
- [x] c. Schlüsselverwaltung ✔ korrekt.
- [x] d. Datenverschlüsselung ✔ korrekt
- [x] e. Authentisierung ✔ korrekt

Die Antwort ist richtig

Die richtigen Antworten sind: Authentisierung, Datenverschlüsselung, Schlüsselverwaltung