Best Practices
Wirkungsvolle Verwendung von FQDNs in Firewall Policies

Thomas Fleischmann

Senior Sales Engineer, Central Europe
Thomas.Fleischmann@watchguard.com

Agenda

- Welche Vorteile hat die Verwendung von FQDN innerhalb einer Richtlinie
- Wie werden FQDN innerhalb der Firebox verwendet
  - Neuerungen in der Version 12.2
- Beispiele aus der Praxis
- Live Demo

Vorteile

- Mit jedem voll qualifizierten Domain-Namen (FQDN = Fully Qualified Domain Name) kann ein beliebiges physisches oder virtuelles Objekt weltweit eindeutig adressiert werden.

- Der FQDN *www.watchguard.com.* ergibt sich durch:

  3rd-level-label. 2nd-level-label. Top-Level-Domain. root-label

  und lautet damit

  www. watchguard. com.

  - Der root-label ist immer leer und wird somit nicht angegeben.

Vorteile

- Als Subdomain bezeichnet man eine Domain, welche in der Hierarchie unterhalb einer anderen liegt. Im allgemeinen Sprachgebrauch sind damit meist Domains in der dritten oder einer weiteren Ebene gemeint.

- Zur logischen und physischen Trennung von Diensten innerhalb der Domain einer Organisation werden traditionell Sub-Domains, z. B. *www.watchguard.com* für den Webserver oder *mail.watchguard.com* für den Mailserver verwendet.
  - Dies ist aber nur eine Konvention!

Vorteile

- Die Nutzung eines FQDN ermöglicht es der Firebox,
  - dynamisch Änderungen bei IP Adressen
  - lokale Auflösungen von Diensten
  - Eindeutige Bestimmung von Dienstanbieter

  durchzuführen, ohne das der Administrator aktiv sich um die Zuordnung von IP Adresse zu einer DNS Name kümmern muss.

Firebox

- Mit der Version 12.2 wurde die Anwendung von FQDNs in der Firebox grundlegend überarbeitet.

- ✓ Sie können jetzt einen Wildcard-FQDN mit mehrstufigen Subdomänen verwenden
- ✓ Mehr als ein FQDN kann nun zu derselben IP-Adresse aufgelöst werden
- ✓ Sie können denselben FQDN in mehr als einer Richtlinie verwenden
- ✓ FQDN-Unterstützung für SNAT

FQDN-Subdomänen Wildcard Unterstützung

- Multi-Level Wildcard-Subdomänenunterstützung für FQDNs in Richtlinien, Aliasnamen und allen Funktionen, die FQDN-Eingaben unterstützen
- Bisher nur 2 Ebenen unterstützt (* .example.com)
- Jetzt mehrstufige Unterstützung bis zu einem theoretischen Maximalwert von 126 für Wildcard-FQDN und 127 Stufen für FQDN mit vollem Namen
- Beispielsweise können Sie jetzt einen Platzhalter-FQDN wie folgt angeben:
  * .beispiel.com
  * .a.beispiel.com
  * .a.b.beispiel.com

- Unterstützt maximal 255 IPs für jeden FQDN

FQDN Wildcard Unterstützung

- Überlappende Adressen in FQDN-Platzhaltern werden nach Richtlinienrangfolge aufgelöst
- Zum Beispiel gilt *a.b.example.com* für alle drei dieser FQDN-Einträge:
  - *** .beispiel.com**
  - *** .b.beispiel.com**
  - **a.b.beispiel.com**
- Die angewendete Richtlinie basiert auf der Prioritätsreihenfolge der Richtlinie
- Wenn eine Richtlinie mit dem FQDN ** .beispiel.com* zuerst in der Richtlinienreihenfolge angezeigt wird, gilt "*a.b.beispiel.com*" für diese Richtlinie

Mehrfache FQDN-Auflösung zu einer IP-Adresse

- Mehrere FQDNs können zu derselben IP-Adresse aufgelöst werden

  Beispielsweise:

  * *.blog.beispiel.com*
  * *.beispiel.com*

- Zuvor hat Fireware die IP-Adresse nur dem ersten FQDN zugeordnet, der zu ihr aufgelöst wurde
  - Dies führte zu Einschränkungen, da FQDNs an vielen Stellen in der Konfiguration verwendet werden können

- Jetzt kann eine IP-Adresse mehr als einem FQDN zugeordnet werden
- Der FQDN, der in traffic log messages angezeigt wird, hängt von der Richtlinienpriorität ab

FQDN in mehreren Richtlinien

- Derselbe FQDN kann in mehr als einer Richtlinie verwendet werden
- Dies verhindert Probleme mit mehreren FQDN-Übereinstimmungen in verschiedenen Funktionen auf Paketebene, z. B.
  - Paketfilterrichtlinien,
  - blockierte Websites und
  - Ausnahmen für blockierte Websites
- Priorität der Richtlinienreihenfolge entscheidet über die FQDN-Auflösung

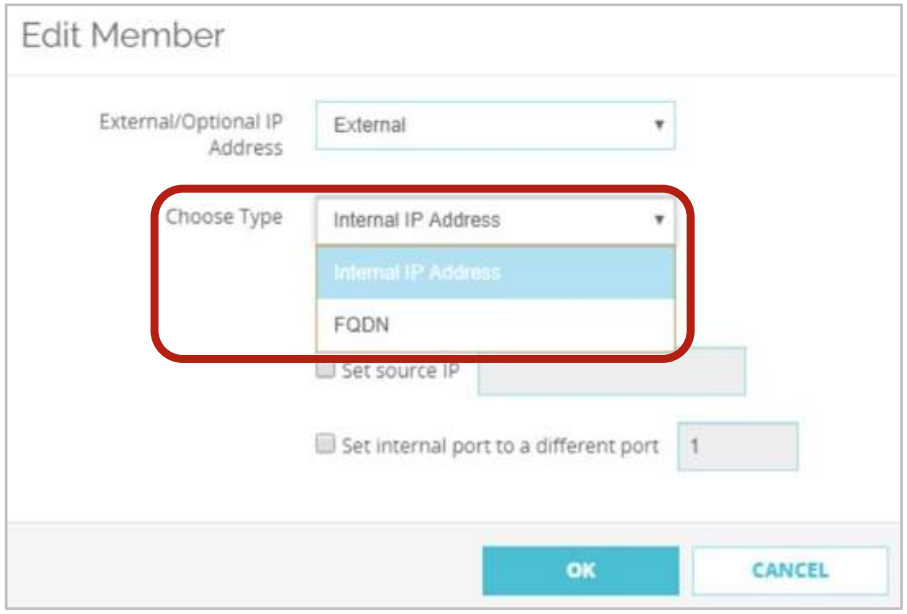
FQDN Support für SNAT

- Sie können nun einen FQDN in einer statischen NAT-Aktion (SNAT) angeben, um die Richtlinienverwaltung zu vereinfachen und Ausfallzeiten aufgrund von IP-Adressänderungen zu vermeiden

- Wenn Ihre Firebox beispielsweise für die Verarbeitung von SMTP-Datenverkehr von einem Office 365-Mail-Server konfiguriert ist, können Sie anstelle von IP-Adressen für Office 365 einen FQDN angeben
  - Wenn sich die Office 365-IP-Adressen ändern, müssen Sie den SNAT-Eintrag nicht mehr aktualisieren

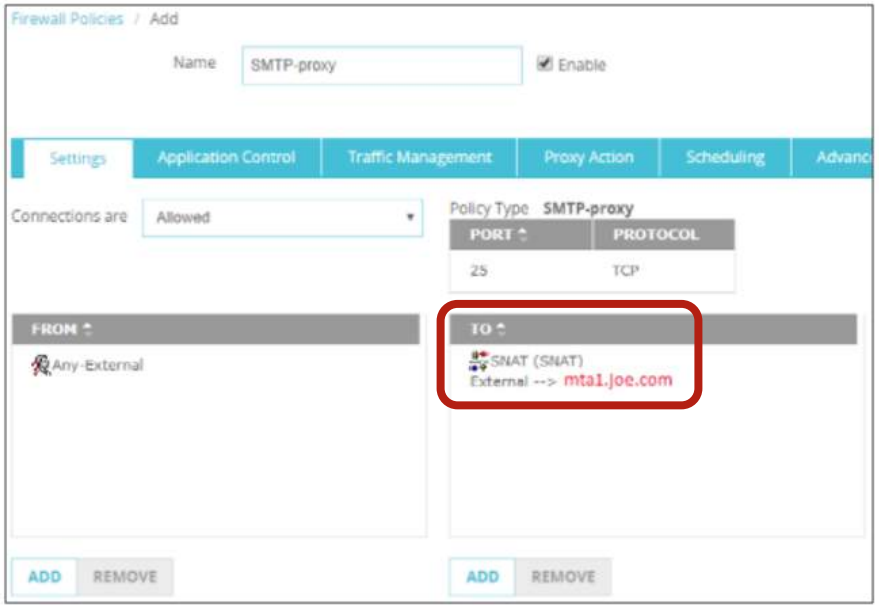
FQDN Support für SNAT

- Wenn Sie ein SNAT-Mitglied hinzufügen oder bearbeiten, wird eine neue Dropdown-Liste mit einer FQDN-Option angezeigt:



FQDN Support für SNAT

- Beispiel - Hybrid-Mail-Umgebung mit einem lokalen Mail-Server und Office 365 in der Cloud
  - Konfigurieren Sie auf der Firebox eine SMTP-Proxy-Richtlinie für Port 25-Datenverkehr von der externen Schnittstelle
  - Fügen Sie einen SNAT-Eintrag hinzu, der einen FQDN für den Office 365-Mail-Server angibt



Voraussetzung / Einschränkung

- Wenn Sie in der Konfiguration FQDNs verwenden, müssen Sie DNS auch auf der Firebox konfigurieren, damit die Firebox die Domänennamen auflösen kann.

Domain Name Auflösung

- Wenn Sie in Ihrer Konfiguration einen Domänennamen definieren, führt Ihre Firebox die DNS-Vorwärtsauflösung für die angegebene Domäne aus und speichert die IP-Adresszuordnungen.
- Bei Wildcard-Domains wie ** .watchguard.com* führt das Gerät die DNS-Auflösung auf *watchguard.com* und *www.watchguard.com* aus.

Voraussetzung / Einschränkung

- Um die durch ** .watchguard.com* implizierten Subdomains aufzulösen, analysiert die Firebox DNS-Antworten, die Ihrer Domain-Name-Konfiguration entsprechen.

- Wenn der DNS-Verkehr die Firebox durchläuft, speichert er die IP-Adresszuordnungsantworten auf relevante Abfragen. Es werden nur **A- und CNAME-Datensätze** verwendet. Alle anderen Datensätze werden ignoriert.

Voraussetzung / Einschränkung

Einschränkungen!

- Beachten Sie diese Einschränkungen, wenn Sie Domänennamen verwenden:
  - Der DNS-Server, der zum Auflösen von Domänennamen verwendet wird, ist der erste statische DNS-Server in Ihrer Konfiguration oder der erste DNS-Server, wenn Ihre Firebox DHCP oder PPPoE auf der externen Schnittstelle verwendet.
  - Nur IPv4-Adressen werden unterstützt!
  - Sie können insgesamt bis zu 1024 Domänennamen konfigurieren, einschließlich Richtlinien, Alias-Mitglieder, Blocked Sites, Ausnahmen für Blocked Sites und Quota-Ausnahmen.
  - Jede Domäne kann bis zu 255 IP-Adressen zuordnen. Ältere IP-Adressen werden gelöscht, wenn das Maximum erreicht ist.

Voraussetzung / Einschränkung

Konfigurationshinweise

- Berücksichtigen Sie bei der Konfiguration von Domänennamen folgende Punkte:
  - Ein Domänenname kann mehreren IP-Adressen entsprechen. Es ist möglich, dass unterschiedliche DNS-Server je nach geographischem Standort, Zeitzone, Lastausgleichskonfigurationen und anderen Faktoren unterschiedliche IP-Adressantworten zurückgeben können.
  - Eine bestimmte IP-Adresse kann mehreren Domänennamen zugeordnet werden. Wenn eine Domäne in eine IP-Adresse aufgelöst wird, entspricht dies einer Firewall-Richtlinie mit dieser bestimmten IP-Adresse in der Richtlinie.

Voraussetzung / Einschränkung

Konfigurationshinweise

- Wenn eine andere Domäne oder Unterdomäne ebenfalls in dieselbe IP-Adresse aufgelöst wird, entspricht der Datenverkehr zu oder von dieser Domäne ebenfalls dieser Richtlinie.
- Dies kann zu Komplikationen führen, wenn Sie für jede Domäne oder Platzhalterdomäne unterschiedliche Zugriffsaktionen konfigurieren. Das verwendete FQDN-IP-Mapping wird durch die Verarbeitungspräzedenz bestimmt:
  - Blockierte Site-Ausnahmen
  - Blockierte Websites
  - Richtlinien (basierend auf der Richtlinienreihenfolge)

Voraussetzung / Einschränkung

Konfigurationshinweise

- **Derselbe FQDN kann in mehreren Richtlinien verwendet werden**
  - Die Richtlinienkonfiguration verhindert Probleme mit mehreren FQDN-Übereinstimmungen, die in verschiedenen Funktionen auf Paketebene auftreten, z. B. Ausnahmebedingungen für blockierte Websites, blockierte Websites und Richtlinien.
  - FQDNs werden durch die Richtlinienpriorität aufgelöst.

Voraussetzung / Einschränkung

Konfigurationshinweise

- **Mehrere Domain-Namen für die gleiche Website**
  - Viele Website-Hauptseiten ziehen Daten von anderen Websites und Second-Level-Domains für Bilder und andere Informationen.
  - Wenn Sie den gesamten Datenverkehr blockieren und eine bestimmte Domäne zulassen, müssen Sie auch alle weiteren Domänen zulassen, die von der Seite aufgerufen werden.
  - Die Firebox versucht, IP-Adressen aus Domänen der zweiten Ebene für eine Platzhalterdomäne zuzuordnen, um den vollständigen Inhalt für eine Site bereitzustellen.

No Go – Was nicht geht

- Folgende Verwendungen von Wildcards werden nicht unterstützt:
  - *.net or *.com (Die Liste der IP-Adresseinträge wäre zu groß für die Verarbeitung)
  - *.*.example.com
  - example*.com
  - *. example.*.com
  - example.*.com

Beispiele

- Ermöglichen Sie den Zugriff auf Softwareupdateseiten wie *windowsupdate.microsoft.com* oder Antivirus-Signaturaktualisierungswebsites, obwohl der gesamte andere Datenverkehr blockiert ist.

- Blockieren oder erlauben Sie den Zugriff auf bestimmte Domains.

- Blockieren Sie den Datenverkehr für eine bestimmte Domäne, erstellen Sie jedoch eine Ausnahme für eine Subdomäne.

Beispiele

- Verwenden Sie den HTTP-Proxy für den gesamten Web-Datenverkehr, umgehen Sie jedoch den Proxy für Content-Delivery-Netzwerke wie * *.akamai.com*.

- Verwenden Sie unterschiedliche Proxy-Richtlinien für verschiedene Domänen. Beispielsweise können Sie eine Proxy-Richtlinie für *example.com* verwenden und eine andere Proxy-Richtlinie für *example2.com* verwenden.


Live Demo